Projet d'audit de flux multimédia	Fluxoip

Définition du besoin

Vous êtes stagiaire à la DSI de la Maison des Ligues de Lorraine (M2L).
Les sites de la maison des ligues vont bientôt disposer d'une infrastructure commune de ToIP (Telephony over IP) et de caméras de surveillance IP – La ToIP est déjà en test pilote dans les bâtiments C et D du site historique.
Le système de téléphonie devra permettre des communications téléphoniques internes, y compris inter-sites. Les caméras surveilleront des endroits sensibles (halls d'entrée, salles techniques …) sur la base de détection de mouvements et de datation.
Le prototypage est en cours sous le nom de projet `Fluxoip` et votre mission va consister à auditer et documenter la solution.

Mission

La mission de votre équipe consistera à :

- Tester (avec preuves) l'accès aux services de téléphonie et de vidéo-surveillance et leur bon fonctionnement, à travers l'infrastructure réseau.
- Documenter l'utilisation de ces services pour leurs futurs utilisateurs.
- Auditer la sécurité des flux et préconiser des solutions si nécessaire.

Pour ce projet en équipe, vous travaillerez en mode `Agile` à l'aide de l'outil `Trello`.

Projet : **AP1.2R**	Contexte : **M2L**	Mode : **projet**	Équipe : **4 étudiants**	Durée : **12 heures**

Cahier des charges

Rendez-vous à la section `Ressources` pour toute documentation complémentaire rassemblée par la DSI pour ce projet.

Les fichiers générés, récupérés ou produits, constitueront des éléments de preuve appréciables.

Infrastructure de Labo

Le travail sera effectué dans l'infrastructure de Labo SISR, rassemblant les éléments de prototypage pour ce projet. Elle comporte :

- un réseau `toip` en `192.168.60.0/24` offrant les services de ToIP (Asterisk SIP+RTP+RTCP), de configuration IPv4 dynamique (isc-dhcp-server DHCP), et de site Intranet (Apache HTTP) depuis le serveur en `.253`.
  Ce réseau est isolé et vous sera uniquement accessible en WiFi.
- un réseau `sio` en `192.168.51.0/24` offrant une palette de services dont ceux de relais de configuration IP dynamique et de passerelle vers Internet en .254, de caméras IP en `.238` (`cam-0` en b100) et `.239` (`cam-1` en b101) et de dépôts de conservation des vidéos collectées ainsi qu'une palette d'autres services (messagerie SMTP+POP3, transfert de fichiers FTP, consultation de vidéos RTSP, …) en `.240` (`nas-0` en b100) et en `.241` (`nas-1` en b101).
  Ce réseau est accessible en filaire (interface de MH `eth0 RT`) et fournit un accès Internet opérationnel.

Vous travaillerez avec les services relatifs à votre salle de Labo.

Afin de pouvoir accéder à ces réseaux, vous aurez besoin par équipe, des hôtes suivants, tous en configuration IP dynamique :

- `toip` (7 téléphones par plot)
  - softphone sur smartphone : 4 (un chacun, en sans-fil, avec l'app `Zoiper` installée)
  - softphone sur VM Win10 : 2 STA nommées et renommées – `sta-tel-113` pour celle installée en salle b101/poste13 – (avec une interface filaire en pont Realtek et une interface sans-fil USB, et Zoiper installé)
  - hardphone avec le téléphone de plot Cisco : 1 (en filaire, précâblé mais à alimenter)
- `sio` (4 STA d'administration par plot)
  - VM Kali : 4 STA nommées et renommées – `sta-adm-113` pour celle installée en salle b101 /poste13 – (une chacun, en filaire en pont Realtek)

Le softphone `Zoiper` a été choisi pour le prototypage, car il est fiable et multiplateforme.

Vous devrez documenter cette infrastructure de Labo par un schéma réseau logique faisant apparaître les éléments cités ci-dessus et pertinents pour votre plot de Labo. Ceci est une priorité !

Téléphonie

L'équipe de développement travaille en parallèle sur une application Web liée à la téléphonie, disponible à l'adresse http://192.168.51.237. Elle est liée au serveur de téléphonie (Asterisk) et fournit notamment un annuaire téléphonique, mais aussi d'autres fonctionnalités. Une fiche de compte d'accès à cette application vous sera fournie individuellement. Cette appli est pour l'instant servie dans les 2 réseaux `toip` et `sio`. Vous pourrez y accéder avec un navigateur de votre MH.

Pour une bonne compréhension du système de téléphonie, tous les participants au projet `Fluxiop` doivent installer le softphone sur leur smartphone et utiliser le système téléphonique en s'appelant mutuellement au moins une fois. Pour cela, vous devrez accéder à votre compte sur l'appli Web maison et vérifier les points suivants :

- Fiche individuelle de compte (vérifier que l'annuaire et la fiche affichée sont cohérents) ;
- Annuaire téléphonique et liste des téléphones connectés ;
- Journaux d'appels (qui peuvent constituer des éléments de preuve…).

Vous devrez aussi contacter votre boite vocale, le numéro qui donne l'heure, celui qui donne l'adresse IP du serveur, et vérifier que le hardphone de votre plot fonctionne bien.
Notez cependant que pour des raisons de performances sur l'infra de Labo, vous devrez prendre un jeton d'accès auprès du prof. de salle.

Afin de simplifier les installations ultérieures, une documentation technique de configuration du softphone sur STA devra être réalisée à destination de l'équipe Infra de la DSI.

Les téléphones obtiennent tous une configuration IP dynamique. Il paraît qu'une procédure technique opérée directement sur les téléphones Cisco permet de récupérer les éléments de cette configuration obtenue par l'hôte. Vous devrez trouver et tester cette procédure, puis la documenter à destination de l'équipe Infra de la DSI. Ce document devra aussi indiquer une procédure d'accès à la configuration du téléphone ainsi que sa sauvegarde et sa restauration.

Zoiper sera aussi déployé sur certains postes utilisateur de la M2L, utilisé avec un casque audio. Vous devez valider que cela fonctionne bien. Pour cela, vous devrez utiliser les 2 clés USB WiFi disponibles dans chaque plot afin de pouvoir connecter les 2 STA Win10 au réseau ToIP. Les 2 qui feront ces tests utiliseront leurs identifiants téléphoniques précédemment utilisés sur smartphone. Les tests doivent montrer que ce client peut appeler une autre STA, un smartphone et le téléphone Cisco.
Dans le cadre de l'audit, il vous est demandé d'effectuer une capture de flux lors d'une conversation téléphonique, à l'aide de l'outil Wireshark.
A partir de ce fichier de capture, vous devrez déterminer le codec utilisé par le système de téléphonie pour encoder et compresser le flux ToIP, ainsi que la bande passante moyenne utilisée par le flux ToIP de votre conversation et le comparer à d'autres sources indicatives (que vous citerez).
Vous devrez vérifier si Wireshark permet de rejouer la conversation à partir du flux capturé, et s'il est possible d'exporter cette conversation pour une lecture ultérieure avec l'outil Audacity.
La conversation téléphonique devra respecter un dialogue préétabli où chacun des interlocuteurs donne son prénom et son nom lors du protocole habituel de communication téléphonique commençant par ‘'allo, bonjour ...''.

Au terme de cet audit, quelles préconisations techniques pourriez-vous faire concernant la sécurité et la confidentialité des flux téléphoniques ?

Vidéo-surveillance

Toutes les tâches relatives au réseau de vidéosurveillance `sio` s'effectueront sur STA d'administration. Toujours dans un souci de sensibilisation des stagiaires à la DSI de la M2L et de polyvalence sur les projets en cours et les technologies associées, tous les membres d'équipe devront avoir une STA d'admin chacun et réaliser au moins une tâche chacun relative à ce réseau.

- **Accès direct à la caméra IP**

Vérifiez que la caméra IP de votre salle de Labo est bien en activité en vous y connectant à l'aide d'un navigateur de votre STA admin afin d'y afficher l'image perçue (prendre un jeton d'accès auprès du prof. de salle).
Comme test de bon fonctionnement et de calibrage, vous vérifierez l'amplitude de vision de la caméra et fournirez en preuve une copie d'écran des 4 angles extrêmes (haut-gauche jusqu'à bas-gauche en sens horaire), ainsi qu'une preuve de votre manipulation avec votre plot et équipe dans le cadre de l'objectif. Inspectez dans votre navigateur l'élément de page Web correspondant à l'image envoyée par la caméra, et trouvez une URL permettant d'afficher directement et en pleine page Web l'image dans votre navigateur.

Vérifiez à l'aide du client VLC qu'il est possible de récupérer le flux vidéo directement sur la caméra IP (à l'aide du code d'accès mobile). Quel est le format de fichier ? Vérifiez si vous avez du son. Enregistrez ce fichier depuis VLC (preuve).

Effectuez une capture Wireshark durant la lecture par VLC du flux vidéo de la caméra IP.
Analysez et déterminez le codec utilisé par la caméra IP pour encoder et compresser les flux vidéo.
Trouvez un moyen de rejouer les flux vidéo et audio dans Wireshark et de les exporter pour lecture ultérieure avec VLC.

Au terme de cet audit, quelles préconisations techniques pourriez-vous faire concernant la sécurité et la confidentialité des flux vidéo ?

- **Accès aux services déportés sur le NAS**

La caméra `Cisco WVC 210` offrant une palette limitée de services en dehors de l'utilisation d'un client dédié (non-adapté aux besoins de la M2L), il a été décidé d'exploiter des services déportés par API disponible dans l'écosystème de l'OS `Synology DSM`, autrement dit sur le NAS `ds110j`.
Les flux vidéo de surveillance par détection de mouvements sont actuellement récupérés et stockés sur un le NAS de vidéosurveillance, avec quelques services associés. Chaque détection de mouvement déclenche un enregistrement minimum de 2 minutes et le fichier correspondant, horodaté, est enregistré sur le NAS.
Un service FTP est aussi actif sur ce NAS, afin de donner accès aux enregistrements vidéo.
Un service de messagerie (SMTP+POP3) est également actif sur l'OS du NAS. Il héberge les boîtes email des ligues, ainsi qu'une boîte email de vidéosurveillance.

Vous vérifierez à l'aide du client VLC qu'il est possible de récupérer le flux RTSP fourni en miroir par le NAS, y compris avec le son. Analysez et trouvez les flux RTP vidéo et audio, les codecs utilisés, ainsi que la bande passante moyenne utilisée par ces flux.
Trouvez un moyen de rejouer les flux vidéo et audio dans Wireshark et de les exporter pour lecture ultérieure avec VLC.

Vous utiliserez le client FTP `Filezilla` pour vous connecter au `nas-0` ou `nas-1` pour récupérer les enregistrements présents.

Vous installerez et configurerez le client de messagerie `Claws` sur votre STA d'administration et accéderez à la boite email de vidéosurveillance.

Les caméras Cisco et leur API Synology ne fournissent pas de système d'alerte liée à la détection de mouvements. Or ceci est un besoin pour la M2L. Deux équipes utilisent le système de vidéosurveillance : la réception de la M2L et l'équipe Infra de la DSI. Elles doivent pouvoir être alertée. Un service de SMS est à l'étude, mais pour l'instant, une boite email est dédiée à cet effet.
Il a été décidé de créer un script (`bash`) exécuté à intervalles réguliers (`cron`), qui consultera le dossier des vidéos de surveillance (`ftp`), calculera le nombre de fichiers et le comparera à la variable d'environnement `nbVideos`, que vous aurez créée. Le cas échéant, un email sera envoyé (`telnet`) à la boîte de vidéosurveillance au service SMTP, avec pour objet "`<nom de la caméra> # <nombre de vidéos> / Eq<n>`" où <n> est le numéro de votre équipe, et comme expéditeur la même adresse que le destinataire.
Tout élément de fichier de configuration ou ligne de script devra être commenté (date, auteur, explication). Cette dernière tâche est complexe pour vous et devra être découpée de manière agile et réalisée par contribution de l'ensemble des membres de l'équipe.

Tâches et livrables

Afin de réaliser ce projet, vous devrez, au sein de l'équipe, planifier et distribuer les **tâches** telles que, par exemple :

- l'identification et la validation des US auprès de la MOA ;
- le découpage des US en tâches d'une durée max de 2h ;
- l'utilisation de `Trello` comme outil de gestion agile du projet, selon la démarche indiquée (rappel dans les ressources) ;
- la répartition des rôles et la distribution des tâches au sein de votre équipe, en respectant les contraintes indiquées par la DSI de la M2L ;
- la spécification de l'infrastructure de prototypage dans le cadre de votre plot de Labo SISR, sous la forme d'un schéma réseau logique ;
- l'importation éventuelle, la mise en réseau et la configuration des hôtes requis pour accomplir votre mission, et la preuve de leur nommage et renommage corrects ;
- toute autre tâche qui découlera de votre analyse du cahier des charges ...

Les **livrables** attendus par la MOA sont :

- **PARTIE GESTION DE PROJET**
  - vos 3 screenshots Trello de fin de chaque séance ;
  - vos journaux de bord ;
  - **Une fiche recette** recensant :
    - la grille synthétique de recette indiquant ce qui est fonctionnel (vert), ce qui est partiellement fonctionnel (orange) et ce qui n'est pas livré (rouge) ;
    - **réserves** : une explication obligatoire pour les modules orange et rouges – par exemple les problèmes rencontrés (techniques, humains, temporels, organisationnels) et les solutions mises en œuvre ou envisagées ;
  - un bilan d'équipe avec 1 à 5 points clés sur :
    - ce que vous avez appris ;
    - ce que vous feriez différemment si c'était à refaire.

- **PARTIE TECHNOLOGIQUE**
  - schéma logique correspondant à votre plot
  - document structuré rassemblant les preuves (copies d'écran) du nommage et renommage de chaque `sta-tel`, et de chaque test de téléphonie avec zoiper (16 preuves dont 4 journaux d'appels)
  - documentations techniques relatives à la téléphonie (2 docs)
  - script de dialogue et preuve de lecture
  - fichier de capture filtré et fichier son exporté
  - analyse encodage et bande passante et préconisations sécurisation flux téléphonie IP
  - document structuré rassemblant les preuves (copies d'écran) du nommage et renommage de chaque `sta-adm`, et de chaque test de vidéosurveillance en accès caméra par navigateur, vlc, wireshark (17 preuves)
  - fichier de capture filtré et fichier vidéo et fichier son exportés
  - analyse encodage et bande passante et sécurisation flux caméras IP
  - documents de preuves (copies d'écran) de chaque test d'accès nas de vidéosurveillance (3 preuves)

- script bash et config cron
- preuve email généré et log d'exécution de script

Tous les documents réalisés sont attendus au format ''universel'' standard **.pdf** – sauf pour les fichiers techniques (fichier de configuration, de capture, audio, vidéo, de script, ...).
Le chef d'équipe rassemble les livrables de ses coéquipiers pour livraison à l'échéance. Les livrables contribuent conséquemment à la note de projet.

Ressources

Un annuaire pour votre classe sur la téléphonie maison vous a été fourni pour y retrouver votre compte.

- login / mdp : `votre login sur l'annuaire / azerty`
- mot de passe secret et messagerie téléphonique : `1234`

Les appareils virtuels à importer (Win10-2019 et Kali-2019) sont disponibles sur votre MH dans `C:\MVORG`. Accès aux VM Win10 (`sisr/P@55aran`) et Kali (`sisr/P@55aran`)

Vous avez également à disposition les ressources suivantes, sur le NAS `Z` :

- `I:\AP\contextes\contexteSIO_M2L\` ;
- `I:\AP\AP1.2r\ressources\` { Docs Labo LSR , Rappels Trello Agile , Docs techniques des téléphones Cisco SPA 301 et des caméras IP Cisco WVC 210 , … } ...

Les applications suivantes devront être installées sur la STA Admin avec `apt` en CLI ou `Synaptic` en GUI : • Application VLC (https://www.videolan.org/vlc/) ;

- Client de messagerie Claws (https://www.claws-mail.org/downloads.php?section=downloads) ; • Le client FTP FileZilla (https://filezilla-project.org/download.php?type=client) est déjà installé. Accès au réseau de Téléphonie (SSID / Clé) : `toip-sio / 510-sisr`

Accès à la caméra IP :

- login / mdp : `siosisr / Passe21`
- code d'accès mobile RTSP : `Passe21`

NAS de vidéosurveillance `nas-0` et `nas-1` :

- boite email : `ipcam.supervision@lorraine-sport.net`
- login / mdp : `siosisr / Passe21`
- URL RTSP (pour les ipCam respectivement des salles b100 et b101) : vous sera fournie dans le fichier `Jeton-equipe<numéro_d_équipe>.txt` dans les ressources. Il sera du type
  ipc100 → `rtsp://admin:<code-d-accès>@192.168.51.240:554/Sms=1.unicast`
  ipc101 → `rtsp://admin:<code-d-accès>@192.168.51.241:554/Sms=6.unicast`

Dossiers FTP : `/videos/ipc100/` et `/videos/ipc101/`