DOCUMENT DE CADRAGE DE LA SAE24

Projet intégratif :

Interception téléphonique

VERSION 1.0 DU 7 JUIN 2022

1. Introduction

LA SAÉ24 est une SAÉ dite intégrative de fin de première année. Elle permet, dans un même projet, de vérifier que vous avez bien acquis une grande partie des apprentissages critiques des 3 compétences de première année :

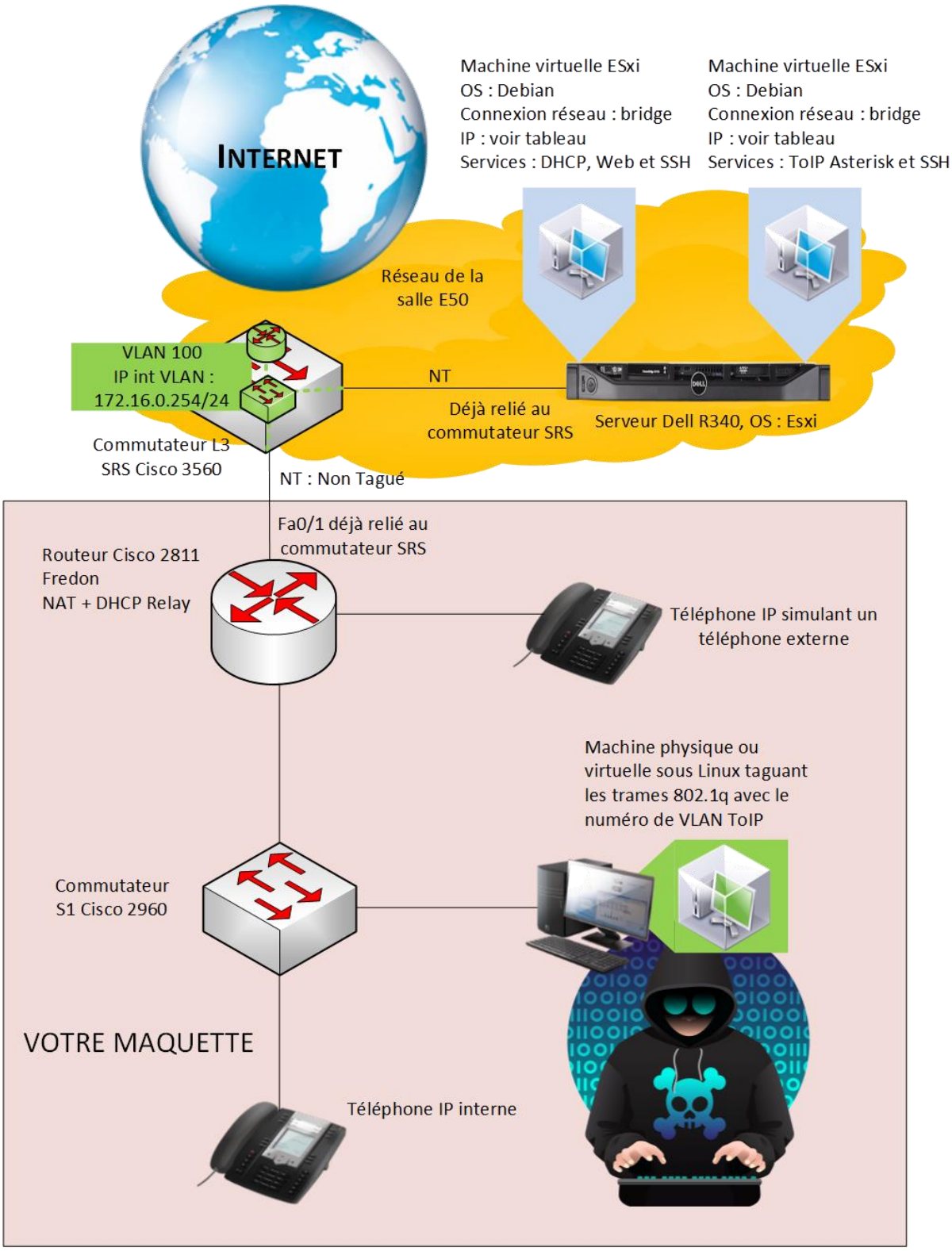
- Administrer les réseaux et l'Internet
- Connecter les usagers et les entreprises
- Créer des outils et application informatiques pour les R&T

En plus des connaissances techniques que vous devrez démontrer, cette SAÉ a pour but de vérifier que vous avez acquis ou de vous faire acquérir les bases de 4 compétences fondamentales pour le travail en entreprise :

- **Faire preuve d'autonomie** : vous serez beaucoup moins guidés pour cette SAÉ et devrez donc faire preuve d'autonomie pour la mise en œuvre de vos réalisations techniques
- **Résoudre des problèmes** : tout au long de cette année, dans vos TP et SAÉ, les enseignants vous ont guidés et expliqués comment isoler et résoudre un problème. A vous maintenant de démontrer que vous avez compris la méthode et êtes capable de la mettre en œuvre !
- **Gérer un projet** : jusqu'à présent dans les SAÉ, les enseignants vous ont donné les différentes étapes détaillées que vous deviez réaliser et le timing à adopter. Il est temps de commencer à voler de vos propres ailes ! Alors pour cette SAÉ, à vous de vous répartir les tâches dans votre binôme et de proposer le timing qui vous semble pertinent.
- **Travailler en équipe** : pour l'instant vous avez toujours travaillé en binôme. Les projets dans une entreprise sont souvent gérés par des équipes de plus grande taille. Pour cette SAÉ vous serez donc une équipe de 6 étudiants. Ce travail en équipe impliquera donc 2 nouvelles tâches : les **réunions d'équipes** pour faire des points d'étapes sur le projet, et les **tests d'intégration** pour intégrer le travail des différents binômes et en faire un projet commun unique. Un enseignant responsable sera désigné **chef de projet** et c'est à lui que vous devrez rendre compte.

2. Objectifs et organisation générale de la SAÉ

Objectifs de la SAÉ 24 : La SAÉ 24 « interception téléphonique » porte sur la réalisation d'une maquette pour illustrer l'interception d'une communication téléphonique après une attaque Man-In-The-Middle MITM entre un téléphone IP et sa passerelle. L'objectif est d'enregistrer les communications téléphoniques sous la forme d'un fichier .wav. L'infrastructure réseau utilisée pour mettre œuvre l'interception sera la suivante :


INTERNET
Machine virtuelle ESxi
OS : Debian
Connexion réseau : bridge
IP : voir tableau
Services : DHCP, Web et SSH
Machine virtuelle ESxi
OS : Debian
Connexion réseau : bridge
IP : voir tableau
Services : ToIP Asterisk et SSH
Réseau de la salle E50
VLAN 100
IP int VLAN :
172.16.0.254/24
NT
Déjà relié au commutateur SRS
Serveur Dell R340, OS : Esxi
Commutateur L3
SRS Cisco 3560
NT : Non Tagué
Fa0/1 déjà relié au commutateur SRS
Routeur Cisco 2811
Fredon
NAT + DHCP Relay
Téléphone IP simulant un téléphone externe
Machine physique ou virtuelle sous Linux taguant les trames 802.1q avec le numéro de VLAN ToIP
Commutateur
S1 Cisco 2960
VOTRE MAQUETTE
Téléphone IP interne

Machine virtuelle	Établi	IP /24
SAE24-Linux-ToIP	1, 3, 7, 11	172.16.0.201
	2, 4, 8, 12	172.16.0.202
	5, 9, 13	172.16.0.203
	6, 10, 14	172.16.0.204
SAE24-Linux-Web-DHCP	1, 3, 7, 11	172.16.0.205
	2, 4, 8, 12	172.16.0.206
	5, 9, 13	172.16.0.207
	6, 10, 14	172.16.0.208
Routeur Fredon (interface Fa0/1)	1 à 14	172.16.0.X (X numéro d'établi)

Login et mot de passe pour les machines virtuelles SAE24-Linux-ToIP et SAE24-Linux-Web-DHCP :

- Login : etudiant ; mdp : SAER&T24 (pour la connexion SSH, pas possible en root)
- Login : root ; mdp : SAER&T24

Nombre d'étudiants par groupe de SAÉ : La SAÉ comprend 3 parties distinctes faites pour 6 étudiants (3 binômes). Pour vous aider à choisir la partie que vous souhaitez traiter, on indique ci-dessous les compétences associées à chaque partie :

- Binômes 1 : Mise en place du réseau
  - Infrastructure Réseau : ☆☆☆☆☆
  - Services réseaux (ToIP, DHCP, Web) : ☆☆☆☆☆
  - Système (virtualisation, Linux) : ☆☆☆☆☆
  - Informatique (XML) : ☆☆☆☆☆
  - Sécurité (VLAN) : ☆☆☆☆☆
  - Signal : ☆☆☆☆☆

  Difficulté / autonomie : la plupart des connaissances techniques de cette partie ont déjà été traitées en TP ou en SAÉ 12 et SAÉ 21. Vous ne serez donc que très peu guidé.

- Binômes 2 : Attaque MITM ARP poisoning avec Python Scapy
  - Infrastructure Réseau : ☆☆☆☆☆
  - Services réseaux : ☆☆☆☆☆
  - Système (Linux) : ☆☆☆☆☆
  - Informatique (programmation) : ☆☆☆☆☆
  - Sécurité : ☆☆☆☆☆
  - Signal : ☆☆☆☆☆

  Difficulté / autonomie: vous avez déjà appris à utiliser Scapy pour parser des paquets FTP dans la SAE11. Cette partie n'est pas forcément très complexe et vous serez donc moyennement guidé.

- Binômes 3 : Parsing des messages SIP/RTP avec Python Scapy et enregistrement de la communication téléphonique :
  - Infrastructure Réseau : ☆☆☆☆☆
  - Services réseaux (protocoles SIP/RTP): ☆☆☆☆☆
  - Système : ☆☆☆☆☆
  - Informatique (programmation) : ☆☆☆☆☆
  - Sécurité : ☆☆☆☆☆
  - Signal (numérisation, codec) : ☆☆☆☆☆

  Difficulté / autonomie : vous avez déjà appris à utiliser Scapy pour parser des paquets FTP dans la SAE11. Cependant cette partie est relativement complexe, vous serez donc assez guidé pour la réaliser.

Il y a 40 élèves soit 6 groupes de 6 et 1 groupe de 4 (7 groupes au total). Pour ce groupe l'attaque MITM sera réalisée avec un logiciel sous Kali Linux.

Enseignants responsables : Willy Guillemin (WG : willy.guillemin@iut-velizy.uvsq.fr), Dana Marinca (DM : dana.marinca@iut-velizy.uvsq.fr), Samuel Marty (SM : samuel.marty@uvsq.fr), Sylvain Chevallier (SC : sylvain.chevallier@iut-velizy.uvsq.fr).

Salles pour la SAE : Pour les séances de projet et TP vous utiliserez les salles de TP suivantes :
- Partie mise en place du réseau : salle E48
- Partie MITM ARP poisoning ou parsing SIP : salle E48 (s'il reste de la place) ou E50

Ressources: les ressources qui vous aideront à réaliser cette SAÉ sont :
- Fiche ressource 1 : DHCP options guide using Linux DHCP server
- Fiche ressource 2 : Grandstream SIP device provisioning guide
- Fiche ressource 3 : Grandstream XML configuration file generator user guide
- Fiche ressource 4 : Compléments sur Python et Scapy pour la SAE24
- Fiche ressource 5 : Python, parsing des arguments avec les packages argparse et getopt

Notation :
Vous aurez 2 notes pendant cette SAE : 1 note sur votre **travail en équipe sur 6 points** et 1 note sur votre **travail personnel sur 14 points**. La note de la SAE sera donc la somme de ces 2 notes.

Les éléments qui seront évalués pour le travail en équipe sont :
- Votre **esprit d'équipe** qui est avant tout une **compétence sociale** :
  - Capacité à vous faire comprendre positivement lors de vos échanges avec d'autres personnes. Il faut manipuler à la fois des compétences d'esprit critique, de gestion des conflits et d'empathie, afin de trouver le meilleur équilibre possible dans le travail en commun. On ne crie donc pas sur un collègue si on n'est pas d'accord, s'il ne comprend pas, ou si on a un différent. On dialogue et si cela ne fonctionne pas, on en discute avec son supérieur (ici le chef de projet)

- Capacité à aider ses coéquipiers en difficulté
- Capacité à aller vers les autres en cas de problème. Comme disait un grand magicien “A ~~Pou~~ Vélizy de l’aide sera toujours apportée à ceux qui en font la demande”.
- Capacité à prendre des initiatives sans oublier d’en discuter avec les autres

Enfin, on travaille dans la bonne humeur, c’est toujours plus agréable pour les autres ! Et bien évidemment, on fournit un travail conséquent, on arrive à l’heure pour éviter de mettre en difficulté l’équipe et de créer des tensions ! Votre esprit d’équipe sera évalué pendant les séances encadrées. Cette évaluation a forcément quelque chose de subjectif puisqu’il s’agira du ressenti des enseignants. Pour autant, vous serez soumis au même type d’évaluation en entreprise et vous devez donc vous y préparer.

- Le **respect des réunions d’équipe** et la **qualité des comptes rendus** donnés au chef de projet.
- Le bon **déroulement des tests d’intégration**
- La **cohérence du diaporama et de la soutenance finale** (on ne doit pas voir qu’il s’agit de 3 projets différents)

3. Planning prévisionnel

Cette SAÉ se déroulent la dernière semaine de cours du jeudi 16 juin au vendredi 24 juin. Elle comprend 50h de projet, 11h encadrées et une soutenance de 40 minutes (10 minutes par binôme) et 10 minutes de questions. Le travail à fournir est donc très conséquent avec des journées typiques de 8h00-12h et 13h-18h. On vous conseille vivement de vous avancer pendant le week-end.

C’est l’occasion de valider son année pour ceux qui sont en difficulté, et l’occasion de montrer vos capacités pour ceux qui envisagent des poursuites d’études. Alors donnez-vous à fond, vous ne profiterez que mieux des vacances ! Le planning prévisionnel est donné ci-dessous :

Date	Volume horaire	Travail à réaliser en séance	Encadrant
Semaine du 6 juin	1h de CM	Présentation de la SAE	WG
Avant mardi 14 juin 12h	1h de travail	Envoyer les membres de l’équipe, les binômes dans l’équipe et les tâches choisies à Mr Guillemin responsable de la SAÉ. Mr Guillemin vous indiquera l’enseignant chef de votre projet. Remarque : En cas de problème pour la constitution des groupes ou de la répartition des tâches, envoyer un mail à Mr Guillemin.	Aucun
Avant Mercredi 15 juin 19h	Trouver 3h dans la	Envoyer le planning prévisionnel (responsable : binôme 1) pour chacun des binômes et pour les tests d’intégration à votre enseignant chef de	Aucun

	semaine pour ce travail	projet. Vous indiquerez les tâches qui doivent être réalisées par chacun des membres du binôme.	
Jeudi 16 et vendredi 17 juin	14,5h de projet 3,5h encadrées	Travail en binôme Vendredi 16h-17h : réunion d'équipe, envoi du compte rendu (responsable : binôme 2) avant 17h30 à votre chef de projet Heures encadrées : jeudi 13h30-15h et vendredi 13h30-15h30	WG
Lundi 20 et mardi 21 juin	15h de projet 3h encadrées	Travail en binôme Mardi 16h-17h : réunion d'équipe, envoi du compte rendu (responsable : binôme 3) avant 17h30 à votre chef de projet Heures encadrées : lundi et mardi 13h30-15h	DM, SM
mercredi 22 et jeudi 23	14h de projet 4h encadrées	Travail en binôme Tests d'intégration Heures encadrées : mercredi 13h30-15h et jeudi 13h30-16h00	WG, SC
Vendredi 24 juin matin	3h00 de projet	Finalisation du diaporama et répétition de la soutenance	Aucun
Vendredi 24 juin après-midi	4h30	Soutenance de projet 13h-17h30 (10 minutes par binôme et 10 minutes de questions) avec 3 enseignants	WG, SC, SM
Total	50h00 de projet + 11h encadrées + 4h30 de soutenance		

4. Travail à réaliser en équipe

Après avoir décidé des 6 personnes qui compenseront l'équipe, vous devrez vous répartir les différentes tâches entre les 3 binômes puis les tâches à l'intérieur du binôme. En cas de problème, veuillez contacter l'enseignant chef de projet qui tranchera.

Vous aurez une première réunion d'équipe le jeudi 16 juin au matin pour réaliser le planning prévisionnel du projet et vous devrez rendre ce planning au chef de projet avant 10h. Pour chaque binôme, ce planning devra indiquer une estimation des dates de finalisation des différentes tâches et la répartition entre les membres du binômes (certaines tâches peuvent cependant se faire en commun).

Vous aurez 2 autres réunions d'équipe qui devront donner lieu à un compte rendu envoyé immédiatement après la réunion au chef de projet :

- Le vendredi 17 juin
- Le mercredi 21 juin

Les réunions d'équipe ont 3 objectifs :

- Faire un état d'avancement des différentes parties du projet

- Faire un état des problématiques rencontrées pour que toute l'équipe et le chef de projet puisse éventuellement proposer une solution
- Éventuellement modifier le planning prévisionnel si le projet a du retard (ou de l'avance)
- Éventuellement modifier les groupes de projet notamment si une partie a pris trop de retard

Le travail en équipe peut faire apparaitre des tensions notamment si un membre de l'équipe ne s'investit pas suffisamment. Si vous rencontrer ce type de problème, vous devez en discuter avec l'enseignement chef de projet qui est en charge de résoudre ces problématiques. Inutile donc de laisser ces tensions s'aggraver rendant ainsi impossible le bon déroulement du projet.

5. Travail à réaliser par le binôme 1 : Mise en place du réseau

Objectif : Mettre en place l'infrastructure réseau et les services sur laquelle sera mise en œuvre l'interception téléphonique. L'infrastructure réseau sera segmentée en 4 réseaux IP : 1 pour les serveurs (172.16.0.0/24), 1 pour le téléphone IP externe, 1 pour les PC (associé au VLAN data sur le switch) et 1 pour le téléphone IP interne et la machine attaquante (associé au VLAN ToIP sur le switch). Le serveur DHCP fournira les adresses IP des PC et des téléphones IP et permettra aux téléphones de récupérer leur numéro de VLAN et l'adresse du serveur Web pour le téléchargement de leur fichier de configuration.

Le travail à réaliser est découpé en 2 types de tâches distinctes :
- Tâches prioritaires : il s'agit des tâches à faire en binôme qui sont nécessaires pour l'intégration du travail des 3 binômes. Vous devez avoir finalisé ces tâches avant de passer aux tâches supplémentaires.
- Tâches supplémentaires : il s'agit des autres tâches à faire en binôme qui ne sont pas nécessaires pour l'intégration du travail des 3 binômes. Vous commencerez après avoir finalisé toutes les tâches prioritaires.

A. Tâches prioritaires : mise en place du réseau

1. Choisir du plan d'adressage IP, des VLAN, la configuration des 3 ports utilisés sur le switch, des numéros de téléphones et login / mot de passe des téléphones pour l'authentification sur le serveur de ToIP
2. Réaliser le schéma réseau
3. Configurer le switch et le routeur en fonction du plan d'adressage IP et des VLAN choisis
4. Installer et configurer le serveur Asterisk sur la machine virtuelle
5. Si vous utilisez une machine virtuelle pour le PC de l'attaquant, créer cette machine sur Virtualbox et installer une distribution Linux, raccorder la machine virtuelle à l'interface du PC et configurer l'interface pour taguer les trames 802.1q avec le numéro de VLAN ToIP
6. Configurer manuellement les téléphones IP et faire des tests de connectivité avec des ping

7. Vérifier le bon fonctionnement du service de téléphonie

B. Tâches supplémentaires : provisioning du téléphone IP interne

1. Installer et configurer le serveur DHCP sous Linux avec 2 pools, un pour les PC et l'autre pour les téléphones IP et vérifier le fonctionnement.
2. Installer le serveur Web Apache sur la machine virtuelle et le tester
3. Comprendre le processus de provisioning automatique des téléphones IP GXP1625 à partir d'un fichier XML. Voir les fiches ressources numéro 4 et 5 :
   - Grandstream SIP device provisioning guide
   - Grandstream XML configuration file generator user guide
4. Création le fichiers XML pour la configuration du téléphone IP interne et l'installer sur le serveur Web. Pour générer le fichier XML à partir du fichier texte, vous utiliserez le « windows_xml_configuration_file_generator_v4.1 ».
5. Modifier la configuration du serveur DHCP pour fournir les options DHCP suivantes : numéro de VLAN et l'adresse du serveur http pour le téléchargement du fichier de configuration du téléphone IP (voir la fiche ressource numéro 3 « DHCP options guide using Linux DHCP server »).
6. Tester le provisioning du téléphone IP interne.

6. Travail à réaliser pour le binôme 2 : Attaque MITM ARP poisoning

Objectif : créer un script Python pour réaliser une attaque MITM « Man In The Middle » ARP poisoning entre 2 équipements d'un même réseau IP que l'attaquant (typiquement un équipement et sa passerelle par défaut).

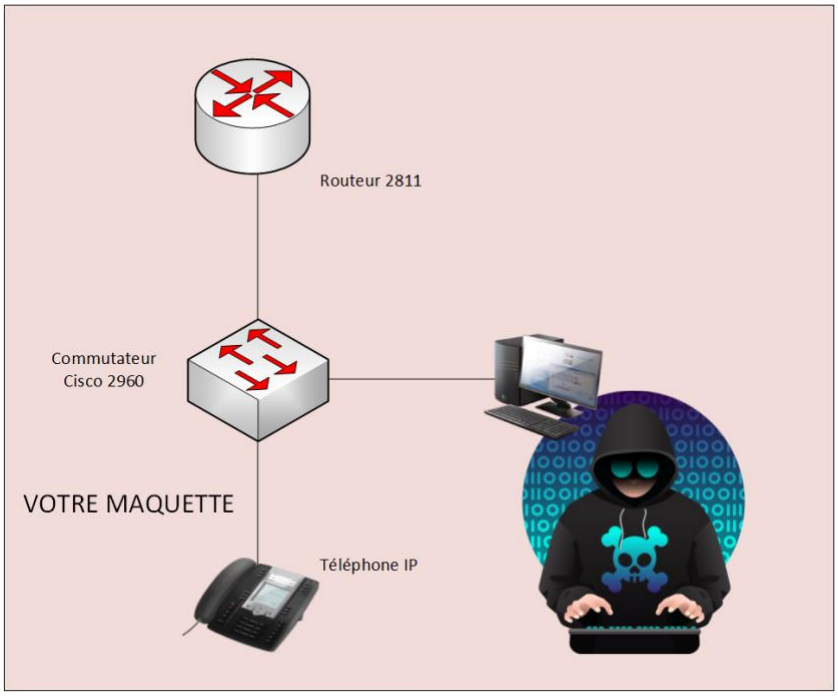
Le script doit être lancé en donnant 3 arguments qui sont les 2 adresses IP des victimes (ici le téléphone et sa passerelle) et l'interface sur laquelle lancer l'attaque. Si une des victimes ne répond pas aux requêtes, la programme se terminera et on l'indiquera dans la console. A la fin de l'attaque on restaurera le cache ARP des victimes pour éviter une rupture des communications et une détection de l'attaque.

A. Tâches prioritaires : attaque MITM ARP poisoning avec Python et Scapy

Le binôme devra :

1. Faire une recherche documentaire pour comprendre le principe de l'attaque ARP poisoning et la décrire avec un schéma dans un notebook.

2. Mettre en place l'architecture de test ci-dessous.



3. Écrire un algorithme (pas de codage à cette étape) dans le notebook décrivant les différentes étapes de l'attaque.

4. Choisir des fonctions qui permettront de réaliser l'algorithme.

5. Se répartir les tâches pour coder les différentes fonctions dans un notebook. Pour chaque fonction, les étudiants décriront pas à pas les différentes étapes de la fonction en les détaillant et les testant pour que la fonction puisse être facilement compréhensible.

6. Coder l'algorithme dans un script pour une machine Linux en s'appuyant sur ces fonctions.

7. Tester le script sur l'architecture de test.

8. Tester le script sur l'infrastructure réalisée par le binôme 1 pour la phase d'intégration.

B. Tâches supplémentaires : gestion des arguments pour lancer le script

On veut améliorer le script en lui fournissant des arguments : adresse IP des 2 victimes avec l'option -v1 pour la victime 1 et -v2 pour la victime 2 et une aide sur l'utilisation de la commande avec -help. Si seul l'option -v1 est donnée, l'attaque se fera entre -v1 et la passerelle par défaut du PC attaquant. Pour réaliser ceci on utilisera le module argparse de Python qui permet de gérer les arguments. Vous trouverez un exemple d'utilisation de argparse dans la fiche ressource 7 « Python, parsing des arguments avec les packages argparse et getopt ».

1. Effectuer la modification du script pour le parsing de la commande

2. Tester votre script.

7. Travail à réaliser pour le binôme 3 : Parsing SIP/RTP

Objectif : une fois l'attaque MITM ARP poisoning réalisée, tous les paquets émis par le téléphone à destination de sa passerelle et les paquets émis par la passerelle à destination du téléphone, vont passer par le PC de l'attaquant.

L'objectif de cette partie est donc de parser (parser : parcourir le contenu de données (ici les paquets reçus) en les analysant pour en extraire des éléments) les messages SIP et RTP qui passent par le PC de l'attaquant pour :

- Détecter le début et la fin d'une communication téléphonique et les paramètres de cette communication
- Enregistrer les données audio transportées dans les paquets RTP dans un fichier .raw (un par sens de communication)
- Convertir à la fin de la communication les fichiers .raw en fichier .wav avec le logiciel sox et fusionner les 2 fichiers pour obtenir la communication téléphonique

A. Tâches prioritaires : parsing SIP/RTP et enregistrement de la communication

Cette partie étant plus complexe que l'attaque MITM ARP poisoning on vous guide un peu plus en vous demandant de coder certaines fonctions. Vous commencerez par travailler sur la capture Wireshark de la communication téléphonique que vous avez dû sauvegarder dans la SAE12.

Les différentes étapes de cette partie sont donc :

1. Analyser la capture Wireshark de la communication téléphonique pour déterminer (travail à faire en commun):
   - Comment identifier l'appelé et l'appelant
   - Quel(s) paramètre(s) retenir pour identifier l'appel
   - Comment identifier les paquets RTP qui transporteront les données audio (pour chaque sens : de l'appelé vers l'appelant et inversement)
   - Comment identifier le codec utilisé

2. Écrire une fonction qui prend comme argument le(s) paquet(s) SIP dans lequel sont indiqués tout ou partie des paramètres de la communication (notamment comment identifier les paquets RTP) et qui retourne ces paramètres.

3. Écrire une fonction convertit les fichiers raw en un fichier wav à l'aide du logiciel de traitement audio en ligne de commande sox. La fonction prendra comme argument le nom des fichiers raw et du fichier wav et les paramètres de codage des échantillons.

   Remarque : On se limitera aux codec u-law et a-law

4. Écrire une fonction qui prend comme argument un paquet RTP et qui ajoute les données audio transportées dans ce paquet à un fichier .raw, un fichier par sens de communication.

5. Écrire une fonction qui prend comme argument le paquet identifiant la fin de l'appel et retourne l'ID de l'appel.

6. A l'aide des fonctions précédentes, écrire, coder et tester dans votre notebook l'algorithme permettant de récupérer dans la capture Wireshark le fichier audio avec la communication.

7. Modifier votre script pour pourvoir récupérer une communication en temps réel en sniffant les paquets sur une carte réseau. Tester votre script sur l'architecture faite par le binôme 1 et après l'attaque MITM ARP poisoning faite par le binôme 2.

B. Tâches supplémentaires

Après ce travail de parsing sur SIP, on propose pour ceux qui ont fini trois 3 types de travail supplémentaire:

1. Vous avez eu du mal à produire ce code et la programmation n'est pas forcément votre tasse de thé. On vous propose alors une recherche documentaire pour expliquer quelles évolutions de SIP et RTP permettent de se prémunir d'une écoute des communications avec une attaque MITM.

2. Vous aimez la programmation, vous souhaitez continuer à travailler sur ce programme. Alors modifiez votre programme pour :
   - Enregistrer dans un fichier texte l'ID de communication, l'heure de début et fin de l'appel et l'identifiant de l'appelé́ et l'appelant
   - utiliser les expressions régulières pour parser SIP. Vous trouverez un cours à cette adresse :
     https://python.sdv.univ-paris-diderot.fr/16_expressions_regulieres/
   - permettre d'enregistrer plusieurs appels en même temps en imaginant que le trafic de plusieurs téléphones passe par votre machine

3. Vous êtes un as de la programmation, cette SAE était vraiment trop facile. D'ailleurs votre maman vous faisait parser du SIP en vous donnant le biberon ! Pas de problème, on vous lâche en totale autonomie :
   - utiliser le module queue pour enregistrer les paquets et créer un stream audio (comme vous l'avez dans la SAE 22) pour diffuser en temps réel la communication téléphonique sur les haut-parleur de votre PC
   - modifier le numéro appelé dans le message INVITE pour rediriger l'appel vers un autre téléphone