BTS SERVICES INFORMATIQUES AUX ORGANISATIONS **SESSION 2025**

Épreuve E6 - Administration des systèmes et des réseaux (option SISR)

ANNEXE 9-1-A : Fiche descriptive de réalisation professionnelle (recto)

DESCRIPTION D'UNE RÉALISATION PROFESSIONNELLE	**N° réalisation : 1**
Nom, prénom : Roelens Gabriel	**N° candidat :**
Épreuve ponctuelle ☐ **Contrôle en cours de formation** ☑	**Date :** ..... / ..... /.....
Organisation support de la réalisation professionnelle	
Intitulé de la réalisation professionnelle	
Période de réalisation : ..... **Lieu :** ..... **Modalité : Seul(e)** ☑ **En équipe** ☐	
Compétences travaillées Concevoir une solution d'infrastructure réseau Installer, tester et déployer une solution d'infrastructure réseau Exploiter, dépanner et superviser une solution d'infrastructure réseau	
Conditions de réalisation[1] (ressources fournies, résultats attendus) • Objectifs du projet : ◦ Déployer une infrastructure de téléphonie IP sécurisée en utilisant Asterisk sur un serveur Ubuntu. ◦ Implémenter des fonctionnalités de filtrage de trafic via IPFire et configurer un pare-feu avec segmentation des flux. ◦ Configurer des services DHCP et assurer la liaison entre les différents contextes utilisateurs (Finance et Comptabilité). ◦ Tester et sécuriser les communications, y compris la mise en œuvre de contre-mesures contre les attaques de type eavesdropping (écoute clandestine). • Ressources attendues : ◦ Installation d'IPFire en tant que pare-feu. ◦ Mise en place de règles de filtrage spécifiques (SSH, HTTP/S). ◦ Configuration d'Asterisk pour gérer les appels SIP, la messagerie vocale et le plan d'appels. ◦ Intégration d'un téléphone IP et mise en place d'une écoute clandestine simulée pour tester la sécurité des communications.	
Description des ressources documentaires, matérielles et logicielles utilisées[2] • Ressources matérielles : ◦ Serveur Ubuntu 20.04 LTS pour l'installation d'Asterisk. ◦ Machine virtuelle (ou physique) pour IPFire en tant que pare-feu. ◦ Téléphone IP (Cisco SPA 303) pour tests pratiques. ◦ Softphones Blink pour simuler les communications SIP. • Ressources logicielles : ◦ Asterisk : serveur de téléphonie IP pour gérer les appels et la messagerie. ◦ IPFire : pare-feu pour la segmentation des réseaux et filtrage des flux. ◦ Wireshark : pour la capture des trames et tester la sécurité. ◦ Blink : softphone pour la gestion des comptes SIP sécurisés. ◦ SIP (Session Initiation Protocol) et RTP (Real-time Transport Protocol) pour la gestion des appels et des flux vocaux. ◦ TLS et SRTP : pour le chiffrement des flux de signalisation et de la voix. ◦ nmap : pour le scan réseau et l'identification des hôtes. ◦ Wireshark : pour observer les flux et tester les attaques MITM.	

[1] En référence aux *conditions de réalisation et ressources nécessaires* du bloc « Administration des systèmes et des réseaux » prévues dans le référentiel de certification du BTS SIO.

[2] Les réalisations professionnelles sont élaborées dans un environnement technologique conforme à l'annexe II.E du référentiel du BTS SIO.

Modalités d'accès aux productions[3] et à leur documentation4

• Accès aux productions :

◦ Les configurations réalisées et les captures de trames sont stockées sur un serveur interne accessible via un espace de stockage dédié.

◦ Documentation complète incluse dans un répertoire partagé sur le réseau de l'établissement. L'accès à ce répertoire se fait via un identifiant et un mot de passe fourni pour le projet.

• Lien vers la documentation complète :

◦ La documentation complète, y compris les schémas réseau, les configurations d'Asterisk, ainsi que les étapes détaillées de mise en place et de tests de sécurité, est disponible sur l'espace de stockage partagé du projet.

BTS SERVICES INFORMATIQUES AUX ORGANISATIONS SESSION 2025

Épreuve E6 - Administration des systèmes et des réseaux (option SISR)

ANNEXE 9-1-A : Fiche descriptive de réalisation professionnelle (verso, éventuellement pages suivantes)

[3] Conformément au référentiel du BTS SIO « *Dans tous les cas, les candidats doivent se munir des outils et ressources techniques nécessaires au déroulement de l'épreuve. Ils sont seuls responsables de la disponibilité et de la mise en œuvre de ces outils et ressources. La circulaire nationale d'organisation précise les conditions matérielles de déroulement des interrogations et les pénalités à appliquer aux candidats qui ne se seraient pas munis des éléments nécessaires au déroulement de l'épreuve.* ». Les éléments nécessaires peuvent être un identifiant, un mot de passe, une adresse réticulaire (URL) d'un espace de stockage et de la présentation de l'organisation du stockage.

[4] Lien vers la documentation complète, précisant et décrivant, si cela n'a été fait au verso de la fiche, la réalisation, par exemples schéma complet de réseau mis en place et configurations des services.

Descriptif de la réalisation professionnelle, y compris les productions réalisées et schémas explicatifs

• Objectifs du projet :

◦ Déployer une solution de téléphonie IP en utilisant Asterisk pour gérer les communications entre deux contextes distincts (Finance et Comptabilité).

◦ Sécuriser les communications via TLS (Transport Layer Security) et SRTP (Secure Real-time Transport Protocol).

◦ Tester la vulnérabilité du réseau via une écoute clandestine (eavesdropping) en simulant une attaque MITM (Man In The Middle).

• Configurations réalisées :

◦ Configuration des comptes SIP dans Asterisk pour les deux contextes, incluant les paramètres de chiffrement TLS pour sécuriser les communications.

◦ Capture des trames avec Wireshark, incluant les résultats de l'appel sécurisé et les tests d'interception.

5. Déroulement du projet

1. Phase 1 : Installation et configuration du serveur Asterisk :

◦ Asterisk a été installé sur un serveur Ubuntu avec la configuration des comptes SIP pour les deux contextes (Finance et Comptabilité).

◦ Mise en place du plan d'appels pour chaque équipe avec des règles de numérotation adaptées.

2. Phase 2 : Mise en place de la sécurité :

◦ Configuration de TLS pour sécuriser le flux de signalisation et de SRTP pour protéger les flux RTP de voix.

◦ Tests des appels SIP chiffrés entre les deux contextes.

3. Phase 3 : Mise en place d'IPFire comme pare-feu :

◦ Configuration d'IPFire pour filtrer les flux réseau et segmenter les différents sous-réseaux pour isoler les communications des deux équipes.

◦ Mise en place de règles de filtrage spécifiques (SSH, HTTP/S) et activation du service DHCP.

4. Phase 4 : Simulation de l'attaque d'écoute clandestine (Eavesdropping) :

◦ Simulation d'une attaque MITM pour tester la vulnérabilité de l'infrastructure avant et après l'activation du chiffrement TLS et SRTP.

◦ Résultats des tests montrant que le chiffrement empêche l'écoute des flux SIP et RTP interceptés.

5. Phase 5 : Sécurisation des communications :

◦ Configuration et validation du chiffrement TLS sur les softphones Blink.

◦ Vérification des certificats via la commande sip show peers dans la console Asterisk.

6. Conclusion

Le projet a permis de déployer une solution de téléphonie IP sécurisée avec Asterisk, intégrant des mécanismes de filtrage des flux via IPFire, la mise en place de règles de sécurité pour le chiffrement des communications (TLS et SRTP) et l'identification des vulnérabilités par des attaques MITM simulées. Les contre-mesures mises en place ont démontré une sécurité efficace contre l'écoute clandestine, et les communications entre les deux équipes sont désormais sécurisées.