Challenge 1 : Craquer des mots de passe

Préambule

L'activité proposée est uniquement à visée pédagogique. Son objectif est l'analyse de failles liées à l'usage de certains protocoles réseaux afin de proposer une amélioration de la sécurité informatique d'un système d'information et de l'hygiène numérique des étudiants. Il permet également l'acquisition de compétences associées au bloc 3 Cybersécurité SISR du BTS SIO.

Les outils abordés dans ce support sont uniquement utilisés à des fins éthiques (Ethical Hacking) et pédagogiques. Leur usage est formellement interdit en dehors de ce cadre sur un réseau tiers sans autorisation explicite.

Pour rappel, l'article 323-1 du code pénal stipule que le fait d'accéder ou de se maintenir, frauduleusement, dans tout ou partie d'un système de traitement automatisé de données est puni de deux ans d'emprisonnement et de 60 000 € d'amende.

Lorsqu'il en est résulté soit la suppression ou la modification de données contenues dans le système, soit une altération du fonctionnement de ce système, la peine est de trois ans d'emprisonnement et de 100 000 € d'amende.

Objectifs

- Scanner un poste / réseau
- Retrouver le mot de passe d'un fichier en se basant sur plusieurs modes d'attaques
- Retrouver le mot de passe d'un utilisateur
- Accéder au compte d'un utilisateur

Logiciels

Vous utiliserez une machine **Kali Linux** pour tester vos attaques.

L'objectif de Kali Linux est de fournir une distribution basée sur Debian regroupant l'ensemble des outils nécessaires aux tests de sécurité d'un système d'information, notamment le test d'intrusion. L'intérêt de Kali Linux est de comporter près de 300 outils déjà installés pour travailler dans le domaine de la cybersécurité.

Des outils de craquage comme "John the Ripper" sont capables de retrouver le mot de passe en se basant sur plusieurs modes d'attaques : Dictionnaire, force brute ou via les tables arc en ciel (rainbow tables).

Nmap est un scanner de ports libre créé par Fyodor et distribué par Insecure.org. Il est conçu pour détecter les ports ouverts, identifier les services hébergés et obtenir des informations sur le système d'exploitation d'un ordinateur distant.

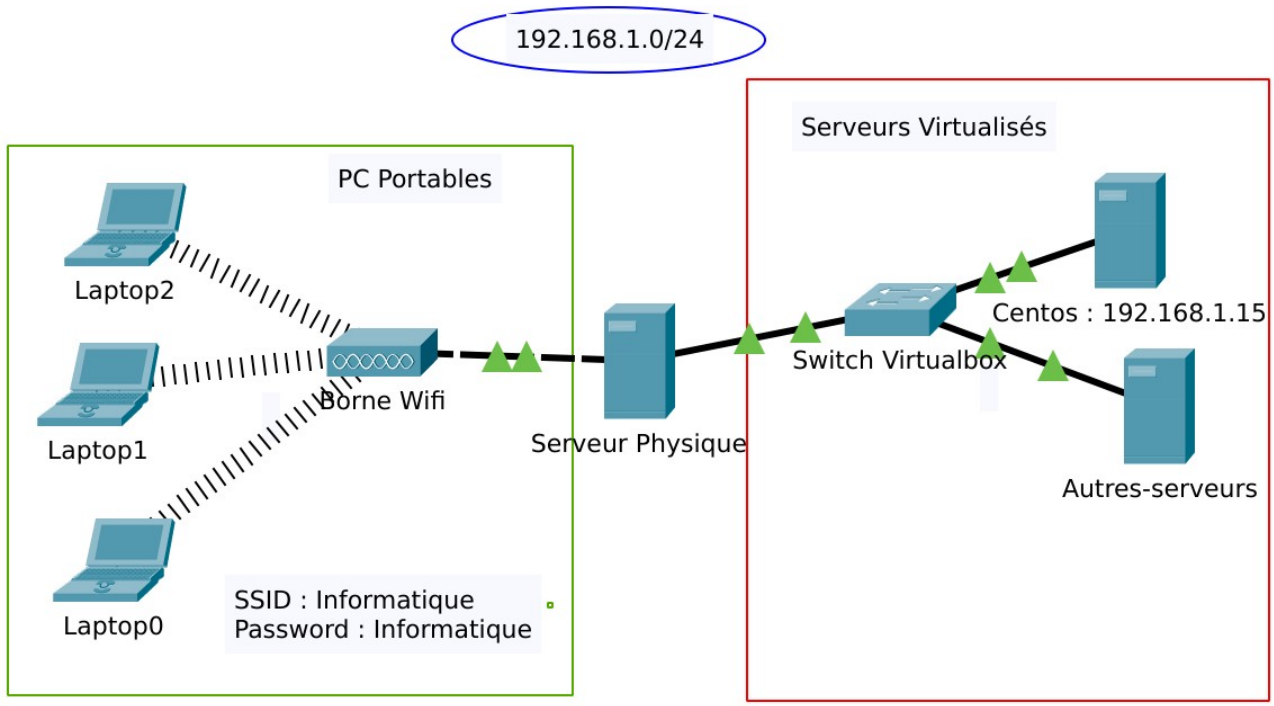
Scénario

Dans ce scénario, chaque groupe de travail tentera de casser des mots de passe de fichiers se trouvant sur le poste Centos.

Pour relever ce challenge, vous devrez découvrir le contenu du fichier final.txt.gpg qui se trouve dans le répertoire personnel du compte eleve de la machine Centos.

Pour accéder au poste Centos, vous devrez vous connecter sur la borne Wifi en utilisant le SSID « Informatique ».

Le schéma du réseau est présenté ci-dessous :



Nous vous invitons à suivre les étapes suivantes :

1. Récupérer le fichier ‘fichier.zip’ sur le compte sio (mot de passe sio).
2. Casser le mot de passe du fichier et afficher le contenu pass.txt.
3. Découvrir le mot de passe de eleve.
4. Récupérer le fichier ‘final.txt.gpg’ sur le compte eleve.
5. Casser le mot de passe du fichier et afficher le contenu du fichier final.txt.gpg.