AC11.05 Savoir identifier les dysfonctionnements du réseau local

Ressources/SAE : R101B R102 R103 SAé1.01 Saé1.2

R1.01b

Contexte

Une infrastructure réseau composée de deux segments principaux a été mise en place :

1. Un réseau local (LAN) avec des PCs, un serveur DNS et un serveur web.

2. Un réseau externe (INTERNET) avec un serveur DNS et un serveur web accessible via un fournisseur d'accès à Internet (FAI).

L'objectif est de vérifier les communications entre les routeurs pour permettre l'accès aux données hébergées sur le serveur WEB situé sur le réseau "INTERNET".

Savoir mis en œuvre

- Connaissance des protocoles de routage pour connecter différentes parties d'un réseau.

- Fonctionnement de serveurs DNS pour la résolution de noms.

- Utilisation des commandes réseau pour vérifier la connectivité entre les segments.

Savoir-faire mis en œuvre

- Configuration des routeurs pour établir une communication entre le réseau local et le réseau externe.

- Vérification de la table de routage sur chaque routeur pour s'assurer que les routes nécessaires sont présentes.

- Test des communications entre les PCs du réseau local et les serveurs du réseau externe.

Savoir-être mis en œuvre

- Rigueur dans la configuration des équipements réseau pour éviter les erreurs.

- Précision dans l'interprétation des résultats des tests de connectivité.

- Collaboration pour documenter les configurations et les résultats.

Tâche réalisée et les résultats

1. Configuration des routeurs :

  - Le routeur `1841 Routeur FAI` a été configuré pour relier le réseau local au réseau externe.

  - Le routeur `1841 Router1` a été configuré pour permettre l'accès au serveur WEB_FAI et au serveur DNS_SFR.

2. Vérification des communications :

  - Une commande `ping` a été utilisée pour tester la connectivité entre :

    - Les PCs du réseau local et le serveur WEB du réseau externe.

- Les serveurs DNS locaux et externes.

- Les tests ont montré une communication réussie entre les deux réseaux.

3. Résolution de noms :

- Les serveurs DNS locaux et externes ont été testés pour s'assurer que les noms de domaine peuvent être résolus correctement.

- Les PCs du réseau local ont été capables de résoudre les noms de domaine des serveurs du réseau externe.

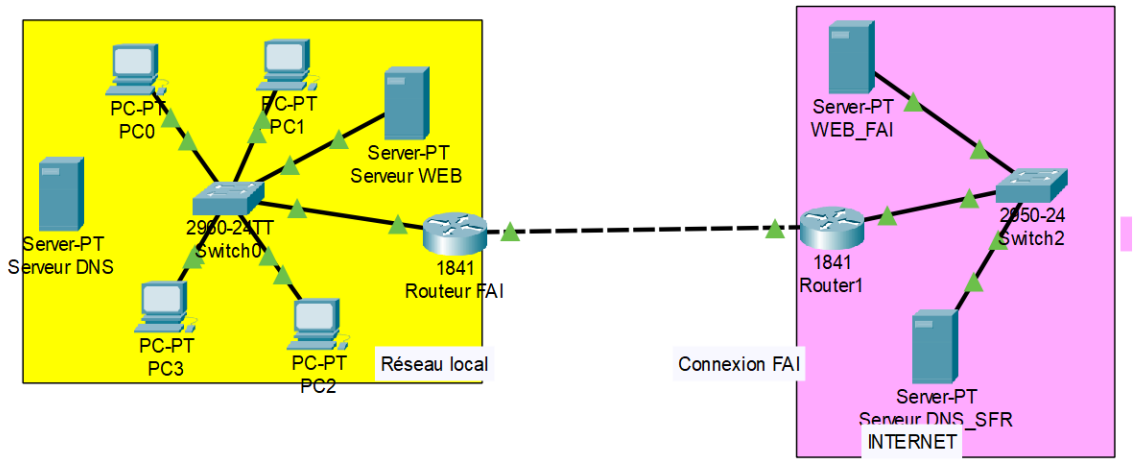
4. Accès au serveur WEB :

- Les PCs du réseau local ont pu accéder aux données hébergées sur le serveur WEB_FAI via un navigateur.

Résultats obtenus

- Une communication stable a été établie entre le réseau local et le réseau externe grâce à une configuration correcte des routeurs.

- Les serveurs WEB et DNS du réseau externe sont accessibles depuis le réseau local.



R1.02

Contexte

Dans le cadre de l'étude du fonctionnement du protocole FTP, une topologie réseau a été mise en place pour se connecter à un serveur et analyser les paquets échangés. Cette analyse permet de mieux comprendre les interactions entre les différentes couches du modèle OSI.

Savoir mis en œuvre

- Connaissance des sept couches du modèle OSI (physique, liaison de données, réseau, transport, session, présentation et application).

- Fonctionnement du protocole FTP (File Transfer Protocol) pour le transfert de fichiers.

Savoir-faire mis en œuvre

- Création d'une topologie réseau avec un client et un serveur FTP.

- Capture des paquets échangés à l'aide d'un outil d'analyse réseau (ex. Wireshark).

- Interprétation des données capturées en fonction des couches du modèle OSI.

Savoir-être mis en œuvre

- Attention aux détails pour l'analyse des paquets capturés.

- Rigueur dans la configuration des équipements et des outils d'analyse.

- Patience et persévérance pour identifier et corréler les informations pertinentes.

Tâche réalisée et les résultats

1. Mise en place de la topologie réseau
   - Un client FTP a été configuré pour se connecter au serveur situé à l'adresse IP `172.16.254.3`.
   - Le serveur FTP est configuré pour répondre aux requêtes FTP et transférer des fichiers.
2. Analyse des paquets capturés
   - Première étape : Le client envoie une requête FTP pour récupérer le fichier `s1-central`.
     - Paquet capturé : `Request: RETR s1-central`.
   - Deuxième étape : Le serveur répond en ouvrant une connexion pour le transfert en mode binaire.
     - Réponse capturée : `150 Opening BINARY mode data connection for s1-central (3100 bytes).`
   - Troisième étape : Le serveur confirme la fin du transfert avec un message de succès.
     - Réponse capturée : `226 File send OK.`

3. Corrélation avec les couches OSI

- Couche application : Protocole FTP pour l'échange des commandes et des données.

- Couche transport : Utilisation du protocole TCP pour garantir la fiabilité de la connexion.

- Couche réseau : Adressage IP pour le routage des paquets entre le client et le serveur.

- Couche liaison de données et physique : Transmission des données sur le support réseau.

Résultats obtenus

- Une connexion FTP fonctionnelle a été mise en place entre le client et le serveur.

- Les paquets capturés montrent clairement les étapes de la communication FTP, du début (requête) à la fin (confirmation de transfert).

- Une compréhension approfondie des interactions entre les couches OSI a été acquise grâce à l'analyse des paquets.

Analyse détaillée des paquets (captures d'écran)

1. Requête FTP (Request: RETR s1-central) :

```plaintext
242 7.709655 172.16.254.3 eagle-server.example FTP 71 Request: RETR s1-central
...
```

- Capture : Le client envoie une requête pour récupérer le fichier `s1-central`.

2. Réponse du serveur (150 Opening BINARY mode) :

```plaintext
246 7.712133 eagle-server.example FTP 124 Response: 150 Opening BINARY mode data connection for s1-central (3100 bytes).
...
```

- Capture : Le serveur ouvre une connexion en mode binaire pour transférer les données.

3. Confirmation de transfert (226 File send OK) :

```plaintext
249 7.712485 eagle-server.example FTP 73 Response: 226 File send OK.
...
```

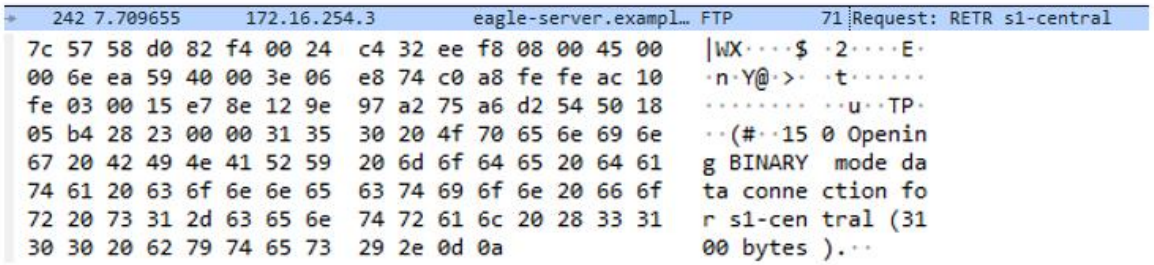
- Capture : Le serveur confirme que le transfert du fichier est terminé avec succès.

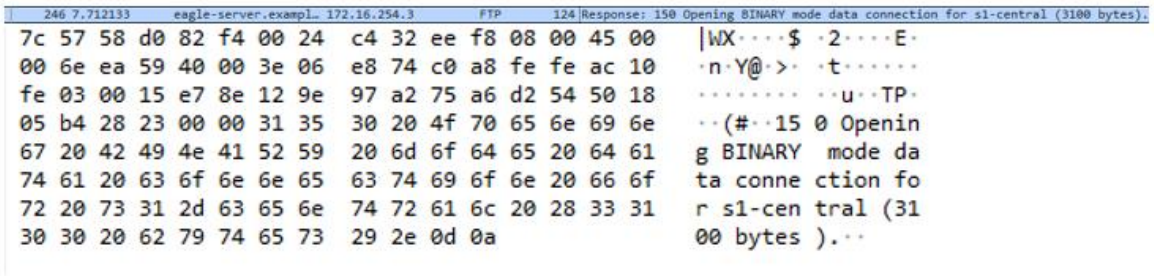
Conclusion

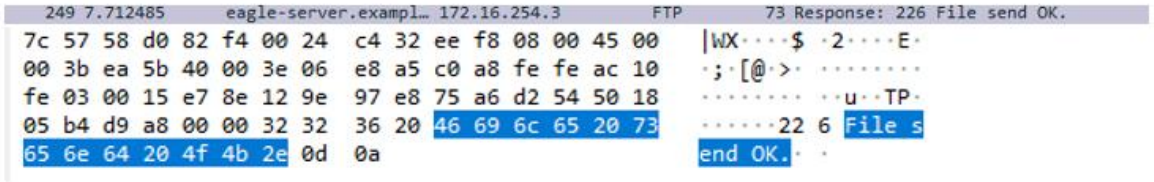
Grâce à cette analyse, les interactions entre les différentes couches du modèle OSI ont été clairement identifiées, et le fonctionnement du protocole FTP a été validé avec succès.

Voici l'analyse de la demande de connexion FTP :

1. Les trois groupes d'unités de données associés au transfert sont :







R1.03

Contexte

Dans le cadre de la surveillance d'un réseau local, une anomalie a été détectée liée à un hôte malveillant. Cet hôte a été identifié grâce à son adresse MAC : `00:0a:f7:8a:00:d6`. Une étude a été réalisée pour localiser cet hôte et identifier le port du switch auquel il est connecté.

Savoir mis en œuvre

- Connaissance des commandes réseau pour l'analyse des adresses MAC.

- Utilisation d'outils comme Wireshark pour capturer et analyser les trames réseau.

- Fonctionnement des tables MAC des switches pour localiser un hôte.

Savoir-faire mis en œuvre

- Analyse réseau avec Wireshark :

  - Identification des trames suspectes contenant l'adresse MAC de l'hôte malveillant.

  - Interprétation des données capturées pour isoler les requêtes et réponses anormales.

- Interrogation des switches :

  - Utilisation de la commande `show mac address-table` pour localiser l'hôte malveillant.

  - Recherche de l'adresse MAC dans la table des adresses du switch pour identifier le port correspondant.

Savoir-être mis en œuvre

- Précision dans l'analyse des trames pour éviter les erreurs d'interprétation.

- Rigueur dans la documentation des étapes suivies pour assurer une traçabilité.

- Réactivité pour minimiser les risques liés à la présence de l'hôte malveillant.

Tâche réalisée et les résultats

1. Analyse avec Wireshark :

   - Capture des trames réseau pour identifier l'hôte malveillant.

   - L'adresse MAC suspecte `00:0a:f7:8a:00:d6` a été mise en évidence dans les trames capturées :

     - Requêtes ICMP (Ping) sans réponse.

     - Trames de diffusion suspectes.

2. Interrogation des switches :

   - La commande `show mac address-table` a été exécutée sur le switch principal (`sw8`).

   - L'adresse MAC `00:0a:f7:8a:00:d6` a été localisée sur le port `Gi1/0/24` (GigabitEthernet 1/0/24) du switch.

3. Vérification du port :

   - Le port `Gi1/0/24` est relié au port Ethernet 3 (`Fa0/11`) sur un autre switch.

   - Cette information a permis de localiser physiquement l'hôte malveillant sur le réseau.

4. Résultat :

   - L'hôte malveillant a été identifié et son emplacement exact dans le réseau a été déterminé.

   - Le port correspondant peut désormais être désactivé ou isolé pour neutraliser l'hôte.

Recommandations

- Renforcer la surveillance réseau pour détecter rapidement les activités suspectes.

- Implémenter des politiques de contrôle d’accès pour limiter les connexions non autorisées.

- Documenter les procédures d’intervention pour les futures occurrences similaires.

Exemple de commandes utilisées

1. Capture des trames avec Wireshark :

  - Filtre utilisé : `eth.addr == 00:0a:f7:8a:00:d6`.

2. Commande pour afficher la table MAC sur le switch :

  ```plaintext

  show mac address-table

  ```

3. Résultat de la commande sur `sw8` :

  ```plaintext

  VLAN    MAC Address       Type       Ports

  ----    -----------       ----       -----

  1       00:0a:f7:8a:00:d6 DYNAMIC    Gi1/0/24

  ```

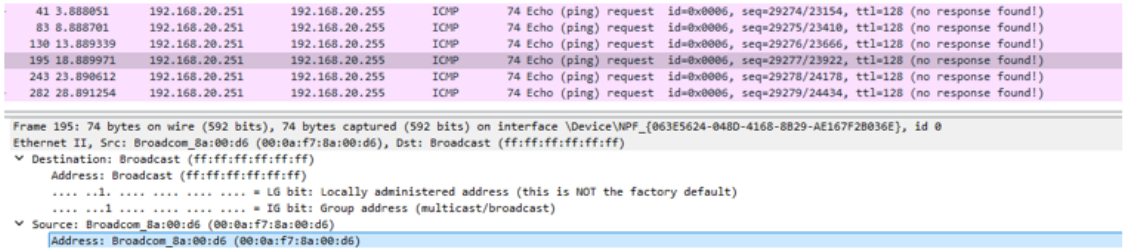
4. Vérification du port Ethernet :

  - Le port `Gi1/0/24` est relié au port `Fa0/11`.

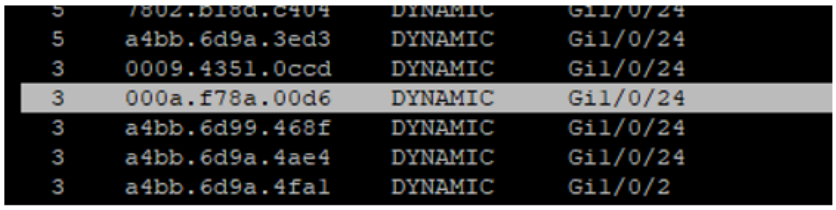
Conclusion

Cette démarche a permis d’identifier et de localiser un hôte malveillant dans le réseau local. Les outils et commandes utilisés ont prouvé leur efficacité pour répondre rapidement à ce type de menace

L’hôte malveillant a pour adresse MAC 00 :0a :f7 :8a :00 :d6



Avec la commande show mac address-table nous avons retrouvé l’adresse MAC de l’hôte malveillant



Sur le terminal de sw8 on utilise la commande show mac address-table.

Puis chercher l’adresse mac précédemment trouvé sur Wireshark et accéder au port qui lui est attribué.

Nous sommes donc aller voir le port 11 sur SW8 et nous avons vu qu’il est relié au port Ethernet 3

SAÉ1.01

Contexte

Dans le cadre d’une recherche documentaire portant sur l’hygiène informatique et la cybersécurité, différentes vulnérabilités rencontrées dans les systèmes informatiques ont été étudiées. Ces vulnérabilités touchent aussi bien les utilisateurs que les infrastructures techniques, et elles mettent en lumière des failles exploitables par des attaquants.

Types de vulnérabilités identifiées

1. Vulnérabilités liées à l'interception et à l'exfiltration

- Fuite d'informations : Capture ou interception des données sensibles lors de leur transfert.

- Attaques de type "Man-in-the-Middle" (MITM) : Interception de données entre deux entités pendant un transfert.

2. Failles dans les mécanismes de chiffrement et protocoles

- Absence de chiffrement ou utilisation de protocoles faibles : Transmission non sécurisée des données.

- Vulnérabilités des VPN mal configurés : Mauvaise sécurisation des tunnels VPN.

3. Vulnérabilités applicatives et humaines

- Logiciels non mis à jour : Failles exploitées en raison de l'absence de mises à jour régulières.

- Vulnérabilités humaines : Manipulation des utilisateurs pour obtenir des informations sensibles (ingénierie sociale).

4. Failles réseau et DNS

- Attaques par déni de service (DDoS) : Surcharge intentionnelle des serveurs ou des réseaux.

- Exploitation des failles DNS : Manipulation des serveurs DNS pour rediriger vers des sites malveillants.

- Absence de segmentation des réseaux : Réseaux non compartimentés favorisant la propagation d'attaques.

5. Vulnérabilités des périphériques et infrastructures connectées

- Appareils connectés peu sécurisés : Périphériques IoT ou systèmes mal protégés.

- Périphériques amovibles non sécurisés : Clés USB ou disques infectés utilisés sans précaution.

- Failles dans les réseaux Wi-Fi : Manque de sécurisation des infrastructures sans fil.

6. Autres attaques ciblées

- Typosquatting : Création de noms de domaines similaires à ceux légitimes pour tromper les utilisateurs.

- Mauvaise gestion des droits utilisateurs : Attribution incorrecte des permissions, permettant à des acteurs malveillants d’exploiter le système.

Recommandations générales pour une bonne hygiène informatique

1. Mettre à jour régulièrement les systèmes et les logiciels pour corriger les failles de sécurité connues.

2. Utiliser des protocoles sécurisés (comme HTTPS et VPN bien configurés).

3. Sensibiliser les utilisateurs aux pratiques de cybersécurité, notamment contre les attaques de type "Man-in-the-Middle" et l'ingénierie sociale.

4. Segmenter les réseaux pour limiter la propagation des attaques.

5. Sécuriser les périphériques connectés et les infrastructures Wi-Fi.

6. Implémenter des systèmes de détection et de prévention des intrusions (IDS/IPS) pour surveiller les activités suspectes.

Conclusion

Cette recherche documentaire met en évidence un large éventail de vulnérabilités dans les systèmes informatiques. Une stratégie efficace de cybersécurité repose sur une combinaison de bonnes pratiques techniques et organisationnelles, ainsi qu'une sensibilisation renforcée des utilisateurs.

SAÉ1.02

Contexte

L'identification et la résolution des dysfonctionnements réseau sont des compétences clés pour garantir la disponibilité et la performance des infrastructures locales. Les problèmes potentiels peuvent inclure :

- Perte de connectivité entre les appareils.

- Problèmes de configuration des VLANs ou des adresses IP.

- Latence élevée ou interruptions intermittentes.

- Défauts au niveau des équipements réseau (switches, routeurs, câbles).

- Mauvaise configuration des services critiques comme DHCP, DNS ou SSH.

Savoirs mis en œuvre

- Comprendre les principes de fonctionnement des réseaux locaux (LAN).

- Maîtriser les outils de diagnostic réseau tels que `ping`, `tracert`, et `tcpdump`.

- Analyser les configurations réseau pour détecter les erreurs.

- Surveiller les performances réseau pour anticiper les problèmes.

Savoir-faire mis en œuvre

1. Diagnostic des problèmes de connectivité

- Vérification de la connectivité via des outils comme :

  - Ping : Pour tester la communication entre deux appareils.

  - Tracert (ou `traceroute`) : Pour identifier les routes réseau et localiser les points de défaillance.

  - Telnet/SSH : Pour tester l'accès à distance aux équipements.

2. Analyse des configurations réseau

- Validation des adresses IP et des sous-réseaux :

  - Vérifier les conflits d'adresses IP dans les VLANs.

  - S'assurer que les passerelles par défaut sont correctement configurées.

- Vérification des VLANs :

  - Identifier les ports mal configurés ou non assignés.

  - Tester les communications entre les VLANs via un routeur ou un switch de niveau 3.

3. Surveillance et tests de performance

- Utilisation d'outils comme Wireshark ou tcpdump pour capturer et analyser le trafic réseau.

- Surveillance des temps de réponse pour détecter les latences.

- Identification des goulets d'étranglement dans le réseau.

4. Vérification des équipements réseau

- Inspection physique des équipements :

  - Vérification des câbles réseau endommagés ou mal branchés.

  - Contrôle des voyants d'état des switches et routeurs.

- Vérification des logs des équipements pour identifier des erreurs ou des alertes.

5. Résolution des problèmes liés aux services critiques

- DHCP : Vérification des baux attribués et des plages d'adresses disponibles.

- DNS : Test de la résolution des noms de domaine.

- SSH : Validation des paramètres d'accès à distance.

Savoir-être mis en œuvre

- Rigueur : Analyser méthodiquement chaque composant pour identifier la source du problème.

- Réactivité : Prendre des mesures rapides pour limiter l'impact des dysfonctionnements.

- Communication : Informer les utilisateurs des problèmes identifiés et des solutions mises en œuvre.

Tâches réalisées et résultats

1. Diagnostic de connectivité :

  - Identification d'un conflit d'adresses IP dans le VLAN 54.

  - Résolution du problème en réattribuant une adresse IP statique.

2. Analyse des configurations :

  - Détection d'un port non assigné au VLAN 105, empêchant la connexion des appareils RH.

  - Assignation corrective du port au VLAN concerné.

3. Surveillance réseau :

  - Capture et analyse du trafic via Wireshark, révélant des paquets en timeout.

  - Réduction de latence en ajustant les priorités QoS sur les switches.

4. Inspection des équipements :

  - Remplacement d'un câble réseau endommagé causant des pertes intermittentes.

  - Mise à jour du firmware d'un switch pour corriger une instabilité.

5. Résolution des problèmes de services :

- Reconfiguration des plages DHCP pour éviter les conflits d’adresse.

- Redémarrage du serveur DNS pour résoudre un problème de cache.

Tutoriel : Utilisation de Wireshark pour analyser le trafic réseau

Installation et configuration

1. Téléchargez et installez Wireshark depuis le site officiel.

2. Lancez l’application et sélectionnez l’interface réseau à analyser.

Analyse du trafic

1. Lancez la capture en cliquant sur "Start".

2. Filtrez les résultats pour détecter des anomalies spécifiques :

- Exemple : `ip.addr == 192.168.1.1` pour surveiller un appareil particulier.

3. Analysez les paquets capturés pour identifier les erreurs ou les délais inhabituels.