AC11.05 Savoir identifier les dysfonctionnements du réseau local

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

R1.01b

Que se passe-t-il ?
Une infrastructure réseau composée de deux segments principaux a été mise en place : un réseau local (LAN) et un réseau externe (INTERNET). L'objectif était de vérifier la communication entre ces deux segments afin de permettre aux PCs du réseau local d'accéder aux serveurs WEB et DNS situés sur le réseau externe.

Comment cela se passe (déroulement, circonstances) ?
Les routeurs ont été configurés pour établir une communication entre le réseau local et le réseau externe. Une vérification des tables de routage sur chaque routeur a permis de valider la présence des routes nécessaires. Des tests de connectivité ont ensuite été réalisés à l'aide de commandes réseau (ping et tests DNS) pour s'assurer que les PCs du réseau local peuvent accéder aux serveurs DNS et WEB situés sur le réseau externe.

Pourquoi cela se passe-t-il ainsi ?
La configuration des routeurs et la vérification des routes sont essentielles pour permettre la circulation des données entre deux segments de réseau. Les tests de connectivité et de résolution de noms garantissent que les configurations ont été réalisées correctement et que les communications entre les deux réseaux sont opérationnelles.

Que peut-on améliorer ?
Il serait intéressant de sécuriser davantage les communications entre le réseau local et le réseau externe en configurant des pares-feux sur les routeurs. De plus, une surveillance continue des performances réseau pourrait être mise en place pour détecter rapidement toute anomalie.

Comment peut-on améliorer ?
En intégrant des outils de monitoring réseau pour analyser le trafic et détecter d'éventuels problèmes. La mise en œuvre de règles de filtrage sur les routeurs pourrait renforcer la sécurité de l'infrastructure.

R1.02

Que se passe-t-il ?
Dans le cadre de l'étude du fonctionnement du protocole FTP, une topologie réseau a été mise en place pour connecter un client à un serveur FTP. Cette expérimentation a permis d'analyser les paquets échangés et de comprendre les interactions entre les couches du modèle OSI.

Comment cela se passe (déroulement, circonstances) ?
Un client FTP a été configuré pour se connecter au serveur situé à l'adresse IP 172.16.254.3. À l'aide d'un outil d'analyse réseau (Wireshark), les paquets échangés ont été capturés. Ces captures ont ensuite été interprétées pour identifier les processus d'échange, depuis la requête initiale du client jusqu'à la confirmation de transfert par le serveur.

Pourquoi cela se passe-t-il ainsi ?
Cette démarche a permis de mettre en pratique les concepts théoriques des couches OSI et de comprendre le fonctionnement du protocole FTP, notamment les étapes d'établissement de connexion, de transfert de données et de confirmation. Cela renforce également les compétences en diagnostic réseau et en interprétation des échanges entre un client et un serveur.

Que peut-on améliorer ?
Il serait intéressant de tester le fonctionnement du protocole FTP dans des scénarios plus complexes, tels que le transfert en mode passif ou actif, et d'analyser les différences dans les captures. De plus, l'intégration de mécanismes de sécurité comme FTPS pourrait enrichir l'analyse.

Comment peut-on améliorer ?
En explorant des configurations avancées du protocole FTP, comme la gestion de sessions simultanées ou le transfert sécurisé via FTPS. L'utilisation d'outils supplémentaires pour analyser les performances réseau, comme le temps de latence ou les éventuelles pertes de paquets, pourrait également offrir une vision plus complète.

R1.03

Que se passe-t-il ?
Une anomalie a été détectée dans le réseau local, liée à un hôte malveillant identifié par son adresse MAC 00:0a:f7:8a:00:d6. Une investigation a été menée pour localiser cet hôte et identifier le port du switch auquel il est connecté.

Comment cela se passe (déroulement, circonstances) ?
L'analyse réseau a commencé par la capture de trames à l'aide de Wireshark, permettant d'isoler les activités suspectes associées à l'adresse MAC de l'hôte. Ensuite, les switches ont été interrogés via la commande show mac address-table pour localiser l'adresse MAC dans leur table des adresses. Cela a permis d'identifier le port Gi1/0/24 sur le switch principal (sw8) comme point de connexion de l'hôte malveillant.

Pourquoi cela se passe-t-il ainsi ?
Cette méthodologie s'appuie sur les outils et protocoles réseaux standards pour identifier les anomalies. L'utilisation de Wireshark et des tables MAC des switches a permis de tracer l'origine du trafic suspect et de localiser physiquement l'hôte malveillant dans le réseau.

Que peut-on améliorer ?
Il serait pertinent de mettre en place des solutions de surveillance proactive pour détecter les activités suspectes en temps réel. De plus, des règles de contrôle d'accès basées sur les adresses MAC pourraient limiter les connexions non autorisées.

Comment peut-on améliorer ?
En intégrant des outils de monitoring avancés comme SNMP ou des systèmes de détection d'intrusions (IDS). La documentation des procédures d'intervention et la formation des équipes sur ces outils amélioreront également la réactivité face à ce type d'incident.

SAÉ1.01

Que se passe-t-il ?
Dans le cadre d'une recherche documentaire sur l'hygiène informatique et la cybersécurité, plusieurs types de vulnérabilités ont été identifiés. Ces vulnérabilités concernent aussi bien la sécurité des transferts de données, des infrastructures techniques, des réseaux, que les comportements humains, et elles mettent en évidence des failles exploitables par des attaquants.

Comment cela se passe (déroulement, circonstances) ?
Les vulnérabilités identifiées se répartissent en six grandes catégories :

1. **Interception et exfiltration** : Capture de données sensibles via des attaques comme les "Man-in-the-Middle".
2. **Failles de chiffrement et des protocoles** : Absence de chiffrement ou utilisation de protocoles obsolètes.
3. **Failles applicatives et humaines** : Absence de mises à jour et ingénierie sociale exploitant les utilisateurs.
4. **Failles réseau et DNS** : Attaques DDoS, exploitation des failles DNS, et absence de segmentation.

5. **Périphériques et infrastructures** : Sécurisation insuffisante des périphériques IoT, clés USB et réseaux Wi-Fi.
6. **Autres attaques ciblées** : Typosquatting et mauvaise gestion des droits utilisateurs.

Pourquoi cela se passe-t-il ainsi ?
Ces vulnérabilités apparaissent en raison de pratiques de sécurité insuffisantes, de l'utilisation de technologies obsolètes ou mal configurées, ainsi que d'un manque de sensibilisation des utilisateurs. Elles exposent les systèmes à des menaces variées, allant de l'interception de données à la compromission complète des infrastructures.

Que peut-on améliorer ?
Pour renforcer la cybersécurité, il est crucial de :

- Appliquer des mises à jour régulières aux systèmes et logiciels.
- Sensibiliser les utilisateurs aux attaques courantes comme l'ingénierie sociale.
- Sécuriser les périphériques IoT et les infrastructures Wi-Fi.
- Mettre en œuvre des mesures de prévention comme la segmentation des réseaux et l'utilisation de systèmes IDS/IPS.

Comment peut-on améliorer ?
En adoptant une stratégie intégrée combinant :

- Des pratiques techniques comme l'utilisation de protocoles sécurisés (HTTPS, VPN).
- Des mesures organisationnelles comme la sensibilisation et la formation des utilisateurs.
- Des solutions technologiques comme des outils de détection d'intrusions pour surveiller les activités réseau.

SAÉ1.02

Que se passe-t-il ?
Dans le cadre de la gestion des infrastructures réseau locales, plusieurs dysfonctionnements ont été identifiés, notamment des conflits d'adresses IP, une mauvaise configuration des VLANs, des pertes intermittentes dues à des équipements endommagés, et des problèmes de configuration des services critiques comme DHCP et DNS.

Comment cela se passe (déroulement, circonstances) ?
Une méthodologie systématique a été suivie pour diagnostiquer et résoudre les problèmes. Les outils de diagnostic réseau tels que ping, tracert, et Wireshark ont été utilisés pour analyser les configurations et surveiller les performances. Les équipements réseau ont été inspectés physiquement, et leurs logs ont été vérifiés pour identifier des erreurs. Enfin, les services critiques (DHCP, DNS, SSH) ont été reconfigurés pour garantir leur bon fonctionnement.

Pourquoi cela se passe-t-il ainsi ?
Ces problèmes surviennent généralement en raison de conflits d'adressage, de configurations réseau incorrectes, ou de défaillances matérielles. Une approche rigoureuse et méthodique est nécessaire pour localiser l'origine des dysfonctionnements et appliquer les correctifs adaptés.

Que peut-on améliorer ?
Il serait bénéfique de :

- Automatiser la gestion des adresses IP avec un serveur DHCP bien configuré.
- Renforcer la documentation des configurations réseau pour éviter les erreurs humaines.