Université Côte d'Azur SI5, parcours CyberSec
Sécurité des réseaux 2022–2023

Examen janvier 2023

Durée : 1 heure 30

Note :

Nom :
Prénom :

L'examen comporte quatre parties indépendantes. Répondez sur la copie avec clarté et concision. Documents autorisés.

1 En bref [5 points]

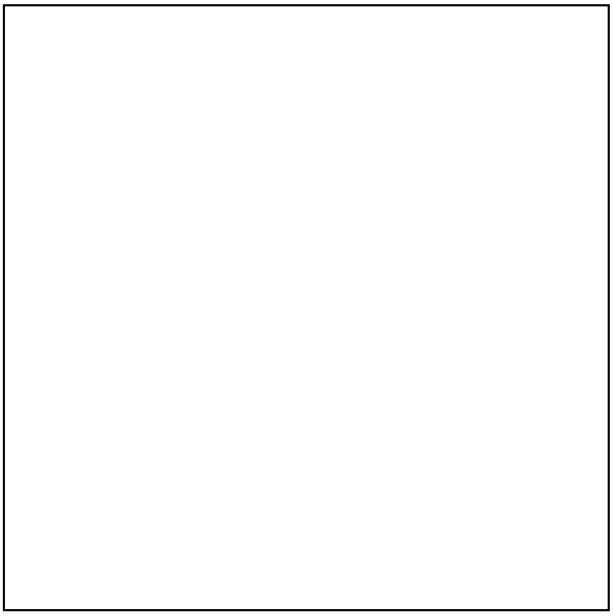
1. Donnez 3 méthodes pour accéder à un service de la `lxle` depuis le côté WAN du routeur.

2. Ettercap permet de réaliser une attaque MIM sur un LAN par modification des tables `arp`. Quel est le service qu'il faudrait attaquer sur un WAN ?

3. Expliquez succinctement la différence entre un DNS resolver et un DNS forwarder.

4. Expliquez et justifiez si OpenVPN comme configuré dans le TP utilise une authentification simple ou à plusieurs facteurs ? S'il y a plusieurs facteurs, lesquels ?

5. Le VPN mis en place en TP est-il en mode pont ou en mode routé (justifiez brièvement) ?



2 Sécurité de SSH [5 points]

Un balayage de la machine `hm.cs.sr` donne le résultat suivant :

```
Starting nmap 7.93 ( http://www.insecure.org/nmap/ ) at 2023-01-19 10:08 CET
Interesting ports on hm.cs.sr (172.16.250.157):
(The 1657 ports scanned but not shown below are in state: closed)
PORT     STATE SERVICE
22/tcp   open  ssh
MAC Address: 00:0B:DB:7A:54:67 (VMWare)
Device type: general purpose
Running: Linux 3.X
Network distance: 1 hop
```

On souhaite contrer une attaque en ligne par tentatives répétées de fournir un couple login/mot de passe généré par un dictionnaire (p.e. au moyen de l'utilitaire `THC Hydra`).
1. Précisez, à la lecture du résultat du scan, si la machine ciblée possède un firewall (et pourquoi).

2. Expliquez succinctement le fonctionnement de cette attaque (et depuis quel réseau).

3. Expliquez comment choisir un utilisateur dont on cherche le mot de passe.

4. Rappelez les principaux modes d'authentification de `ssh` et dites celui que vous privilégieriez pour sécuriser une connexion distante voire contrer l'attaque par recherche de mot de passe.

5. Dites comment contrer cette attaque. Vous pouvez utiliser d'autres programmes que `sshd`. Si vous n'en connaissez pas le nom, décrivez-en le fonctionnement.

3 Analyse d'un rapport de vulnérabilité [6 points]

La capture d'écran ci-dessous présente un rapport de vulnérabilité d'une machine des TP.

Vulnerability	Severity ▼	QoD	Host IP	Host Name	Location
SSL/TLS: Renegotiation DoS Vulnerability (CVE-2011-1473, CVE-2011-5094)	5.0 (Medium)	70 %	172.16.250.157		25/tcp
SSL/TLS: Renegotiation DoS Vulnerability (CVE-2011-1473, CVE-2011-5094)	5.0 (Medium)	70 %	172.16.250.157		143/tcp
Check if Mailserver answer to VRFY and EXPN requests	5.0 (Medium)	99 %	172.16.250.157		25/tcp
SSL/TLS: Deprecated TLSv1.0 and TLSv1.1 Protocol Detection	4.3 (Medium)	98 %	172.16.250.157		25/tcp
TCP timestamps	2.6 (Low)	80 %	172.16.250.157		general/tcp
Services	0.0 (Log)	80 %	172.16.250.157		25/tcp
Services	0.0 (Log)	80 %	172.16.250.157		80/tcp
SSL/TLS: Version Detection	0.0 (Log)	80 %	172.16.250.157		25/tcp

1. Quels sont les services de cette machine identifiés par le scanner ?

2. À votre avis, cette machine a-t-elle été scannée depuis le côté WAN ou depuis le côté LAN ? (Et dites pourquoi).

3. Quels sont les services absents (ou ne présentant pas de vulnérabilité) par rapport aux TP ? Attention, la réponse dépend si vous pensez être du coté LAN ou WAN.

4. Quels sont les risques liés au service `smtp` (port 25) d'envoi de mail et comment s'en prémunir ?

5. Comment la sécurité du service `imap` (port 143) est-elle assurée (rappelez-vous le TP) ?

6. Comment compléteriez-vous cette analyse de vulnérabilité ?

4 Problème d'accès distant [4 points]

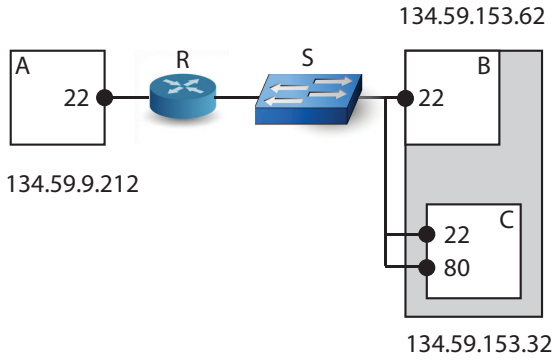


FIGURE 1 – Schéma du réseau.

Selon la Figure 1 on dispose de 3 machines, sur 2 réseaux différents : `134.59.9.0` et `134.59.153.0` qui hébergent, respectivement, la machine `A` et les machines `B` et `C`. Le port 22 (`ssh`) des machines `A` et `B` est ouvert et accessible depuis Internet. Les services (`ssh` et `http`) hébergés sur la machine `C` ne sont accessibles que depuis le réseau `134.59.153.0` (donc pas directement depuis le réseau `134.59.9.0`).

1. Expliquez comment il est possible d'implémenter cette "politique de sécurité" sachant que les réseaux sont reliés par un routeur `R` et que les machines `B` et `C` sont sur un réseau switché par le commutateur `S`. (Il y a beaucoup de réponses possibles !).

2. Un utilisateur (disposant d'un compte utilisateur sur les 3 machines) veut accéder au serveur `http` hébergé sur la machine `C` depuis la machine `A`. Expliquez comment il peut procéder pour lire les pages web hébergées sur `C` depuis `A`. On rappelle que l'utilisateur n'a pas les droits `root` et qu'il ne peut donc pas installer de nouveaux services.