Titre : Dispositifs de sécurité
Contexte : Activité professionnelle N°11

Compétences du bloc 1 :

- **Travailler en mode projet**
  - Analyser les objectifs et les modalités d'organisation d'un projet
  - Planifier les activités

Compétences du bloc 2 :

- Installer, tester et déployer une solution d'infrastructure réseau
- Rédiger ou mettre à jour la documentation technique et utilisateur d'une solution d'infrastructure
- Tester l'intégration et l'acceptation d'une solution d'infrastructure
- Exploiter, dépanner et superviser une solution d'infrastructure réseau
  - Administrer sur site et à distance des éléments d'une infrastructure
  - Gérer des indicateurs et des fichiers d'activité des éléments d'une infrastructure

Compétences du bloc 3 :

- **Sécuriser les équipements et les usages des utilisateurs**
  - Identifier les menaces et mettre en œuvre les défenses appropriées
  - Gérer les accès et les privilèges appropriés
  - Vérifier l'efficacité de la protection
- **Assurer la cybersécurité d'une infrastructure réseau, d'un système, d'un service**
  - Prévenir les attaques
  - Détecter les actions malveillantes
  - Analyser les incidents de sécurité, proposer et mettre en œuvre des contre-mesures

Prérequis :

- Créez le GANTT pour cette nouvelle AP.
- Complétez votre schéma réseau et votre document de synthèse sur les VLANs et VMs créés dans votre environnement.
- Rendre votre document de synthèse avant vendredi minuit au plus tard.
- Tout nouveau serveur devra être référencé par un nom FQDN (DNS), inventorié dans GLPI puis supervisé par Nagios.

1] Contexte

Dans cette nouvelle AP, vous allez mettre en place quelques outils pour assurer un certain niveau de sécurité pour votre environnement menuimétal :

- Connexion distante par **SSH** avec une authentification par clef publique
- Connexion distante par **VPN**
- Mise en place du framework logiciel **Fail2ban**

Questions :

- Parmi la liste des outils énumérés ci-dessus, pouvez-vous les classer selon les critères suivants : IDS, IPS, outil de connexion distante.
- Quelle(s) est/sont la/les différence(s) entre IDS et IPS ?
- Quelle(s) est/sont la/les différence(s) entre SSH et VPN ?
- A partir de quelle source de données fonctionne l'application Fail2ban ?
- Quelle application sera utilisée par fail2ban pour « blacklister » les IPs « malhonnêtes » ?

2] Connexion distante par SSH avec authentification par clef publique

A lire absolument :
https://www.cnil.fr/fr/cybersecurite/comprendre-les-grands-principes-de-la-cryptologie-et-du-chiffrement

Objectif attendu : En suivant les contraintes ci-dessous, vous ferez en sorte de pouvoir vous connecter à vos serveurs Linux GLPI et NAGIOS depuis un client Windows 10 de votre environnement en utilisant une authentification par clef publique.

Puisque vous allez changer la configuration SSH de vos deux serveurs Linux, vous ne pourrez plus y accéder depuis l'application Remina du poste Ubuntu du lycée, vous utiliserez alors si besoin la console Proxmox.

A la fin de l'AP, vous rétablirez la configuration initiale des services SSH de vos serveurs Linux pour pouvoir à nouveau vous y connecter par SSH depuis Remina.

Un « vieux TP » intitulé SIO21_TP_YG_Connexion_SSH_Version_2023_2024.pdf téléchargeable sur Pronote vous permettra d'implémenter une configuration SSH avec ou sans utilisation d'une clef publique.

Contraintes :

- Si nécessaire, installez le service SSH sur les deux serveurs en question et faites en sorte qu'il fonctionne sur le port 2222 et non plus le port par défaut (càd 22).

- Depuis votre VM Windows 10 cliente, vérifiez à l'aide de l'application **nmap** (https://www.it-connect.fr/chapitres/nmap-installation-et-configuration-linux-et-windows/ puis https://www.it-connect.fr/chapitres/nmap-scans-des-ports-tcp-et-udp/) que le serveur SSH des deux serveurs Linux est fonctionnel. Quelle commande, que vous avez déjà utilisée, vous permet de vérifier la même chose directement sur votre serveur Linux ?

- Côté serveur, mettre en place une authentification par clef publique pour vous connecter en SSH depuis un client Windows ou Linux en utilisant l'application Putty (à installer si nécessaire :

  https://www.tutos.eu/3194
  https://www.it-connect.fr/chapitres/authentification-ssh-par-cles/

  - Le couple « clef publique/privée » doit être généré depuis l'application **puttygen** .

  

  - Transférer la clef publique sur votre serveur Linux à l'aide de l'application de votre choix (client FTP Filezilla par exemple !). Il faudra au préalable vérifier que le paquet **openssh-sftp-server** (port 22 ou 2222 si modifié) est installé sur le serveur, c'est normalement le cas si le paquet **openssh-server** est lui-même présent.

  - Depuis votre client Windows ou Linux, testez une connexion vers vos deux serveurs en utilisant l'application **Putty**, vous ferez en sorte de lui indiquer la présence d'une clef privée.

- Faire en sorte que les log d'authentification de votre serveur Linux soit redirigé vers votre serveur **Rsyslog**, classé dans un dossier spécifique bien évidemment !

3] Connexion distante par VPN

A lire absolument :
https://www.cnil.fr/fr/cybersecurite/comprendre-les-grands-principes-de-la-cryptologie-et-du-chiffrement

Afin de répondre aux problèmes de télétravail, le directeur de la société Menuimétal souhaite qu'une connexion VPN depuis l'extérieur soit mise en œuvre pour permettre aux employés de travailler depuis chez eux. Pour différentes raisons, M. Lepage décide de choisir la solution OpenVPN.

Mme Bercy vous demande, en tant que stagiaire, une étude technique afin de démontrer que la solution mettant en œuvre l'outil OpenVPN, est une solution viable pour l'entreprise. Dans votre argumentaire, vous prendrez soin également d'expliquer les termes suivants :

- Confidentialité, intégrité, authentification,
- chiffrement symétrique/asymétrique,
- easy-rsa,
- certificat,
- algorithme Diffie-Hellmann.

De plus, un technicien, Monsieur Yagui 😉, vous fournit également une documentation intitulée « SIO21_TP_YG_OpenVPN_version_2025_2026.pdf » qu'il a rédigée et qui permettra de répondre en partie aux attentes (voir sur Pronote).

Questions :

- Quel port réseau utilise le VPN ? Quel protocole utilise VPN (TCP ou UDP) ?
- Quel type de VPN allez-vous mettre en œuvre (Ethernet ou IP) ?

Objectif attendu :

- Un employé de la société doit pouvoir se connecter au serveur VPN et avoir accès aux différents serveurs du VLAN « LAN ».

Contraintes :

- Pour cela, vous disposez de plusieurs éléments :
  - ☐ Votre environnement Proxmox,
  - ☐ une nouvelle VM jouant le rôle de serveur VPN et hébergée dans votre le VLAN « LAN »,
  - ☐ un client OpenVPN sur une VM Windows 10 connecté au VLAN Invité. Cette configuration servira à simuler un accès virtuel extérieur,
  - ☐ un client OpenVPN sur un ordinateur portable Linux ou Windows connecté au VLAN Invité du commutateur HP de votre banc de travail. Cette configuration servira à simuler un accès physique extérieur.

Tout le trafic du client doit passer par le VPN.

- Pour la connexion VPN :
  - ☐ Le client doit se voir demander un mot de passe lors de l'établissement de la connexion VPN (option **nopass** à ne pas utiliser donc),
  - ☐ depuis le serveur VPN, vérifiez en temps réel qui est connecté au VPN,
  - ☐ depuis le client, vérifiez que vous récupérez les bons paramètres réseaux (IP de votre serveur DNS).

- Faire en sorte que les log d'openvpn de votre serveur Linux soit redirigé vers votre serveur **Rsyslog**, classé dans un dossier spécifique bien évidemment !

4] Fail2BAN

Documentations utiles :

- https://fr-wiki.ikoula.com/fr/Mettre_en_place_fail2ban_sur_Debian
- https://www.it-connect.fr/premiers-pas-avec-fail2ban/
- https://www.webhi.com/how-to/fr/comment-installer-et-configurer-fail2ban-sur-linux/
- http://doc.ubuntu-fr.org/fail2ban
- https://slash-root.fr/fail2ban-installation-et-configuration/
- https://www.linuxtricks.fr/wiki/fail2ban-bannir-automatiquement-les-intrus

Objectif attendu : En suivant les contraintes ci-dessous, surveillez les services SSH de deux serveurs Linux (autres que ceux utilisés dans la partie 2 de cette AP) et bannir les IPs à l'origine de connexions non autorisées (erreur de saisie de mot de passe par exemple).

Contraintes pour chaque serveur :

- Installez l'application **fail2ban**.

- Installez le paquet **iptables** qui permettra à Fai2ban d'agir sur le bannissement des IPs.

- Augmentez le niveau de log à « **Debug** » pour Fail2ban (fichier **/etc/fail2ban/fail2ban.conf** à modifier)

- La configuration de Fail2ban par défaut est définie dans le fichier **jail.conf**, ce fichier est automatiquement modifié lors des mises à jour du service, il est donc recommandé d'effectuer une copie de ce fichier en le renommant **jail.local** puis en le plaçant dans le répertoire **/etc/fail2ban/**

- Faire en sorte que le client Windows 10 autorisé à se connecter aux services SSH ne puisse jamais être banni.

- Modifiez la prison (Jail in English) pour le service SSH (ligne 274 du fichier **jail.local**).
  - Activez la surveillance.
  - Modifiez le port réseau comme voulu précédemment.
  - Ajouter le filtre pour SSH (l'ensemble des filtres existants sont situés dans **/etc/fail2ban/filter.d/**)
  - Bannissez les IP au bout de trois essais infructueux pendant 60 secondes.

- Redémarrez le service Fail2ban puis vérifiez l'état de la prison pour SSH (commandes **fail2ban-client status** et **fail2ban-client status sshd**) voir **tail -f /var/log/auth.log**

- Depuis une autre VM équipée d'un client SSH, tentez une connexion avec un mauvais mot de passe puis vérifiez que son adresse IP est bannie. On peut utiliser les commandes précédentes voire **iptables -L -n -v**

- Vérifiez les logs du service Fail2ban avec **journalctl** ou **tail -f /var/log/fail2ban**

- Paramétrez Fail2ban pour qu'il puisse envoyer un mail à l'administrateur de votre choix lorsqu'une IP est bannie. Testez la réception du mail depuis un client de messagerie.

Pour la gestion des notifications par mail, je vais vous aider … Voilà mes sources malgré tout :

- https://edywerder.ch/fail2ban-email-notification/
- https://bobcares.com/blog/configure-sendmail-to-use-smtp-relay/
- https://linuxconfig.org/sendmail-unqualified-hostname-unknown-sleeping-for-retry-unqualified-hostname
- Et ChatGPT 😉

Ces manipulations sont à réaliser sur les machines où se trouve Fail2ban.

1. Editez le fichier **/etc/fail2ban/jail.local** et modifiez comme suit :

```
171  # ACTIONS
172  # Some options used for actions
173  # Destination email address used solely for the interpolations in
174  # jail.{conf,local,d/*} configuration files.
175  destemail = toto@guillien.lycee
176
177  # Sender email address used solely for some actions
178  sender = fail2ban
179
180  # E-mail action. Since 0.8.1 Fail2Ban uses sendmail MTA for the
181  # mailing. Change mta configuration parameter to mail if you want to
182  # revert to conventional 'mail'.
183  mta = sendmail
```

- ☐ Ligne 175 : Personne qui sera avertie
- ☐ Ligne 178 : Emetteur du mail
- ☐ Ligne 183 : Application de gestion de mail utilisée par défaut

```
257  # Choose default action.  To change, just override value of 'action' with the
258  # interpolation to the chosen action shortcut (e.g.  action_mw, action_mwl, etc) in jail.local
259  # globally (section [DEFAULT]) or per specific section
260  action = %(action_mwl)s
```

- ☐ Ligne 260 : on choisit la valeur **action_mwl**, ce qui permettra de joindre les logs dans le corps du document du mail.

2. Editez le fichier **/etc/mail/sendmail.mc** et modifiez comme suit :

```
107  dnl # Default Mailer setup
108  MAILER_DEFINITIONS
109  FEATURE(`authinfo')dnl
110  MAILER(`local')dnl
111  MAILER(`smtp')dnl
112  define(`SMART_HOST',`[192.168.2.9]')dnl
113  define(`RELAY_MAILER_ARGS',`TCP $h 25')dnl
114  define(`confAUTH_OPTIONS',`A p')dnl
115  define(`confAUTH_MECANISMS',`PLAIN LOGIN')dnl
```

Attention au deux types de quotes utilisées :
- ALTGR 7 soit ` pour la quote inversée du début

- ☐ Ligne 109 : on active l'authentification pour pouvoir transmettre un mail via notre serveur de messagerie **Postfix** déjà en place. Ce dernier va donc nous servir de relais SMTP.

- ☐ Ligne 112 à 115 : on indique l'adresse IP du serveur (ici 192.168.2.9) ainsi que le numéro de port réseau utilisé (ici 25 soit SMTP par défaut).

3. Editez le fichier **/etc/mail/authinfo** et modifiez comme suit :

```
1  AuthInfo:192.168.2.9 "U:titi" "P:titi" "M:PLAIN"
```

- ☐ Ligne 1 : si le serveur SMTP exige une authentification, ce qui est le cas dans notre environnement Menuimétal, nous renseignons les paramètres d'un compte utilisateur de la messagerie qui sert à l'envoi des mails de Fail2ban, ici ce sera l'utilisateur titi
  - Derrière « AuthInfo », nous renseignons l'IP du serveur SMTP de mail.
  - Derrière le « U: », vous indiquerez l'identifiant et après le « P: », vous indiquerez le mot de passe.

4. Indiquez dans le fichier **/etc/hosts** l'IP, le FQDN et le nom de la machine :

```
1  192.168.2.7 SrvNagios.guillien.lycee SrvNagios
2
3  # The following lines are desirable for IPv6 capable hosts
4  ::1     localhost ip6-localhost ip6-loopback
5  ff02::1 ip6-allnodes
6  ff02::2 ip6-allrouters
```

5. Exécutez les commandes ci-dessous pour le service **sendmail** :
- ☐ `makemap hash /etc/mail/authinfo < /etc/mail/authinfo`
- ☐ `m4 /etc/mail/sendmail.mc > /etc/mail/sendmail.cf`
- ☐ `systemctl restart sendmail.service`

Pas d'inquiétude, le redémarrage du service est un petit peu long.
Pour info, il est possible d'examiner les logs en exécutant :
`tail -f /var/log/mail.log`

6. Exécutez les commandes ci-dessous pour le service **fail2ban** :
7. `systemctl restart fail2ban.service`