Documentation de test projets BTS

Fiche de tests

Nous allons maintenant vérifier si toutes les configurations faites précédemment fonctionnent.

Nous procèderons comme ceci:

- 1.Sécurité du réseau avec pfSense, Squid et SquidGuard
- 2. Serveur principal sous Windows Server 2019
- 3. Monitoring réseau avec Nagios
- 4. Gestion de la maintenance avec GLPI
- 5. Postes de travail collaborateurs
- 6. Sauvegarde cloud automatisée avec AWS et PowerShell
- 7. Redondance Active Directory et DNS
- 8. VPN Sécurisé avec OpenVPN
- 9. Surveillance et Sécurité du Réseau
- 9.1. Système de Détection d'Intrusion (IDS/IPS)
- 9.2. Analyse du Trafic avec Wireshark
- 10. Stockage et Partage des Données
- 10.1. Infrastructure NAS avec TrueNAS
- 11. Messagerie d'entreprise via Zimbra

1 –

Tout d'abord nous nous rendons sur les postes de l'étude pour intégrer le certificat précédemment crée dans pfSense

Sélectionner un magasin de certificats	×					
Sélectionnez le magasin de certificats que vo voulez utiliser.	ous					
Personnel Autorités de certification racines de Confiance de l'entreprise	e conf	stème où les o	certificats s	ont cons	ervés.	
Autorités de certification intermédia Éditeurs approuvés Certificats pon autorisés	aires 🗸	un magasin d ificat.	e certificat	s, ou vou	JS	
<	>	sin de certifica	ats en fonc	tion du t	ype de	
OK Ar	nuler	sin suivant				
				Parco	urir	
			Suiva	ant	Annule	r
	_		Suiva	arit	Annule	· ·
	•	OneDrive				
		OneDrive				
Certificat		OneDrive	×			
Certificat énéral Détails Chemin d'accès de certificat	tion	OneDrive	×			
Certificat énéral Détails Chemin d'accès de certificat	tion	OneDrive	×			
Certificat énéral Détails Chemin d'accès de certificat Informations sur le certificat Ce certificat est conçu pour les rôles • Toutes les stratégies d'amissions • Toutes les stratégies d'amissions	tion s suivants	OneDrive :	×			
Certificat énéral Détais Chemin d'accès de certificat Informations sur le certificat Ce certificat est conçu pour les rôles • Toutes les stratégies d'amissions • Toutes les stratégies d'application	ion suivants	OneDrive :	×			
Certificat énéral Détals Chemin d'accès de certificat Informations sur le certificat Ce certificat est conçu pour les rôles • Toutes les stratégies d'application • Toutes les stratégies d'application Délivré à : internal-ca	tion	OneDrive :	×			
Certificat énéral Détails Chemin d'accès de certificat Informations sur le certificat Ce certificat est conçu pour les rôles • Toutes les stratégies d'amissions • Toutes les stratégies d'application Délivré à : internal-ca Délivré par internal-ca	tion	OneDrive :	×			
Certificat énéral Détals Chemin d'accès de certificat Informations sur le certificat Ce certificat est conçu pour les rôles • Toutes les stratégies d'émissions • Toutes les stratégies d'application Délivré à : internal-ca Délivré par internal-ca Valide du 08/11/2024 au 06/11/	2034	OneDrive :	×			
Certificat énéral Détails Chemin d'accès de certificat Informations sur le certificat Ce certificat est conçu pour les rôles • Toutes les stratégies d'émissions • Toutes les stratégies d'application Délivré à : internal-ca Délivré par internal-ca Valide du 08/11/2024 au 06/11/ Installer un certificat	ion suivants	OneDrive : :	X -			

Le certificat est bien intégré, nous pouvons maintenant essayer d'accéder aux sites bloqués

\leftarrow \rightarrow O () https://www.instagram.com		ίê	£'≊	¢	٢	
	-					
	A					
	La connexion de ce site n'est pas sécurisée					R
	www.instagram.com a envoyé une réponse non valide.					
	Essayez d'exécuter les diagnostics réseau Windows.					
	ERR,SSL,PROTOCOL,ERROR					

lci instagram est bien bloqué

Egalement pour Twitch.tv

\leftarrow	C () https://fr.twitch.tv	A»	ŵ
	La connexion de ce site n'est pas sécurisé	e	
	fr.twitch.tv a envoyé une réponse non valide.		
	ERR_SSL_PROTOCOL_ERROR		
	Résolution de problèmes Actualiser		

Egalement whatsapp

← C ()	https://www.whatsapp.com/?l=en	Aø .
	La connexion de ce site n'est pas sécurise	ée
	www.whatsapp.com a envoyé une réponse non valide.	
	ERR_SSL_PROTOCOL_ERROR	
	Résolution de problèmes Actualiser	

2. Serveur principal sous Windows Server 2019

On voit que notre GPO dédié au menu exécuter fonctionne



Ainsi que nos fond d'écrans



Maintenant vérifions les autrisation d'accés aux dossiers sensibles

Ici nous pouvons voir que sophie marin n'a pas accès au dossier tandis que Isabelle Moreau si

8 Sophie SP. MARIN



Ainsi nous bloquons l'accès aux donnés sensible en fonctions des demandes de la cliente.

3. Monitoring réseau avec Nagios

Pour se faire nous allons déconnecter le pc 2 du réseau et ainsi voir si effectivement il apparait comme étant down et donc non fonctionnel sur nagios

La vm est éteinte



Et le pc est répertorié comme down dans nagios

HOST		status • •
AD_DS_Server	8	UP
Windows_PC1	8	UP
Windows_PC2	<u>s</u>	DOWN
localhost	8	UP
pfSense	8	UP

Ainsi que le pc 1

11995		wares -	Last street.
AD_DS_Server	- 🔒	UP	11-22-2024 01:55:22
Windows_PC1	- 🔒	DOWN	11-22-2024 02:00:53
Windows_PC2	- 🔒	DOWN	11-22-2024 01:57:22
localhost	- 🔒	UP	11-22-2024 01:58:22
pfSense	- 🔒	UP	11-22-2024 01:59:22

Ainsi nous pouvons nous assurer du bon état des services et des equipements

4. Gestion de la maintenance avec GLPI

Ξ

Nous allons nous connecter sur le compte glpi de la cliente et créer un ticket de demande support en passant par le raccourcie préalablement appliqué sur le bureau du poste de la cliente.



On arrive sur le compte de la cliente



On crée un ticket

Туре	Incident		*
Catégorie		•	i
Urgence	Très haute		*
Éléments associés	+		
Observateurs	× 8 Moreau Isabelle 🇘	0	
Titre	Déconnection outlook		
Description *	Paragraphe 🗸 🗸	в I	
	Bonjour, depuis ce mai ma messagerie outloo recontacter au plus vit Cordialement.	in 9h je n'ai plus accès∣a ç. Je vous pris de me e.	1,
	Fichier(s) (2	Mio maximum) i	
	Glissez et dépos	ez votre fichier ici, ou	
	Choisir des fichiers	Aucun fichélectionné	

On se rend sur un compte administrateur



Nous avons un ticket

IM	Créé : ① Il y a 4 minutes par 名 Moreau Isabelle Dernière mise à jour : ① Maintenant par 名 gipi Déconnection outlook
	Bonjour, depuis ce matin 9h je n'ai plus accès a ma messagerie outlook. Je vous pris de me recontacter au plus vite. Cordialement.
GL	Créé : O Maintenant par 8 glpl Bonjour, je vais prendre contact avec vous par téléphone pour prendre la main sur le poste. Cordialement Helpdesk

Nous pouvons voir que tout fonctionne correctement, nous pouvons facilement communiquer pour agir le plus rapidement possible pour ainsi débloquer la cliente.

5. Postes de travail collaborateurs

Nous allons nous rendre sur le poste de Sophie Marin pour faire les vérifications nécessaires

La cliente n'est pas administrateur, elle ne peut pas faire ce qu'elle veut sur son poste comme demandé.



Nous allons tenter de mettre le poste en ip fixe par exemple.

Contrôle de compte d'utilisateur × Voulez-vous autoriser cette application à apporter des modifications à votre appareil ?				
Éditeur vérifié : Microsoft Windows Afficher plus de détail				
Pour continuer, tapez un nom et un mot de passe d'administrateur. Nom d'utilisateur				
Mot de passe				
Oui Nan				

La cliente rentre ses identifiants de sessions

Contrôle de compte d'utilisateur	×				
Voulez-vous autoriser o apporter des modificat	Voulez-vous autoriser cette application à apporter des modifications à votre appareil ?				
Connexions réseau					
Éditeur vérifié : Microsoft Window	WS				
Afficher plus de détail					
Pour continuer, tapez un nom et d'administrateur.	un mot de passe				
Nom d'utilisateur					
Mot de passe					
Domaine : TECHNOVALIS					
L'opération demandée nécessite une élévation.					
Oui	Non				

Elle ne peut pas, seule le compte technovalis ainsi que le compte de la Notaire de l'étude peuvent accéder à cette console, donc pour toutes les modifications sur le poste, la cliente devra faire la demande auprès de la notaire.

Bien sur c'est un exemple, une collaboratrice n'irait pas changer l'ip du pc, cependant nous ne pouvons écarter les potentiels erreurs de manipulations.

6. Sauvegarde cloud automatisée avec AWS et PowerShell

Pour ce test nous allons créer des fichiers test, lancer la tache planifiée manuellement et vérifier si ceux-ci apparaissent bien dans le bucket de sauvegarde de l'étude dans AWS.

Lorsque l'on arrive dans le planificateur de tache nous pouvons voir que la tache de 23h s'est bien appliquée

🔘 Inf	21/11/2024 23:10:03	102	Tâche terminée	(2)	b187aeb7-2
() Inf	21/11/2024 23:10:03	201	Action terminée	(2)	b187aeb7-2
🛈 Inf	21/11/2024 23:00:01	200	Opération dé	(1)	b187aeb7-2

Le Planificateur de tâches a terminé l'instance « (b187aeb7-26dd-4cc9-9749-3af165185935) » de la tâche « \Sauveagrde etude moreau » pour l'utilisateur « TECHNOVALIS\i.berrada »

Nous allons essayer avec des fichier text test

TEST 4	12/11/2024 01:03
TEST TEST	11/11/2024 23:15
TEST2	12/11/2024 00:15
test3	12/11/2024 00:52

On lance manuellement la tache

On se rend ensuite dans AWS et nous pouvons observer dans le bucket de sauvegarde de l'étude que les fichiers sont bien sauvegardés dans le cloud

sauvegarde-cloud-etude-moreau Info	test/	(Copier l'URI S3
Objets Propriétés Autorisations Métriques Gestion Points d'accès	Objets Propriétés	
Objets (3) Info	Objets (5) info Image: Compart FURIL 53 Image: Compart FURIL 54 Image: Compart 54 <th>er Ouvrir 🗇 Supprimer pouvez utilier l'<u>inventaire Amazon 53 (?</u> pour prespersonnes puisert accéder à vos objets, composition de la composition de la co</th>	er Ouvrir 🗇 Supprimer pouvez utilier l' <u>inventaire Amazon 53 (?</u> pour prespersonnes puisert accéder à vos objets, composition de la composition de la co
Q. Rechercher des objets en fonction du préfixe	modification modification	16 0 o Standard
□ Nom ▲ Type ▼ Dernière modification ▼ Taille ▼ Classe de stockage ▼	Image: Test state tot 01:59:33 AM CET Image: Test state tot 12 Nov 2024 Image: Test state tot 01:59:49 AM CET	23.0 o Standard
C Actes client/ Dossier	TEST.txt txt 12 Nov 2024 02:00:06 AM CET	8.0 o Standard
Dossier	□ D TEST2.txt txt 12 Nov 2024 02:00:22 AM CET	6.0 o Standard
□ □ <u>test/</u> Dossier	test3.txt txt 11:08:15 PM CET	27.0 o Standard

Nous pouvons remarquer que les sauvegarde sont incrémentielles.

Ainsi, la sauvegarde quotidienne fonctionne sans soucis et sont bien envoyé tout les soir a 23h dans le cloud pour ne pas générer la production.

7. Redondance Active Directory et DNS

En premier lieu nous allons éteindre le serveur principal et voir si le serveur secondaire prend le relais.

```
C:\Users\i.moreau>nslookup technovalis.local 192.168.2.6
Serveur : SRVBACKUP.technovalis.local
Address: 192.168.2.6
Nom : technovalis.local
Addresses: 192.168.2.4
192.168.2.6
```

Il prend bien le relai, maintenant nous allons tenter la modification des identifiant d'un utilisateur.

Réinitialiser le mot de pass	e	?	×
Nouveau mot de passe :	•••••		
Confirmer le mot de passe :	•••••		
L'utilisateur doit changer le session	e mot de passe à la procha	ine ouverture	e de
L'utilisateur doit fermer puis modifications prennent effe État de verrouillage du compt	ouvrir à nouveau sa sessio t. e sur ce contrôleur de dom	on afin que le aine : Déver	es rouillé
Déverrouiller le compte	de l'utilisateur		
	ОК	Annu	uler

Les identifications utilisateur ont bien été modifiés





8. VPN Sécurisé avec OpenVPN

OpenVPN Connect ->				
≡	Profiles	10		
CONNEG	CTED			
	OpenVPN Profile 10.0.2.15 [pfSense-UDP4- 1194-vpnuser1-config (7)]			
CONNEG	CTION STATS			
6.2KB/s		_		
		_		
0B/s		- 1		
BYTES IN 40 B/S	↓ ↑ BYTES C	DUT S		
DURATIO 00:00:1	N PACKET RECEIVED 2 1 sec ago			
YOU		D		

On arrive bien à se connecter à notre server VPN.

9. Système de Détection d'Intrusion (IDS/IPS)

2017-07-22 2 06:15:49	UDP	Potentially Bad Traffic	163.172.17.76 € Q ⊞	54465	Q 🕀	5060	140:26 🕀 🗙	(spp_sip) Method is unknown
2017-07-21 2 09:26:30	UDP	Potentially Bad Traffic	163.172.22.169 Q ⊞	52428	Q 🕀	5060	140:26 🕀 🗙	(spp_sip) Method is unknown
2017-07-21 2 01:03:28	UDP	Potentially Bad Traffic	163.172.17.76 Q ⊞	46834	Q ±	5060	140:26 🕀 🗙	(spp_sip) Method is unknown
2017-07-20 2 20:36:37	UDP	Potentially Bad Traffic	163.172.22.169 S Q ⊞	54788	Q ±	5060	140:26	(spp_sip) Method is unknown

Notre système de détection d'intrusion fonctionne correctement, des alertes commencent à remonter

9.2. Analyse du Trafic avec Wireshark

Analyse du Trafic avec Wireshark

Je lance wireshark sur l'interface Ethernet puis je tente de faire un ping depuis une autre machine.

ICMP 101 Destination unreachable (Port unreachable)

192.168.2.4

La trame icmp du ping remonte bien.

68 8.190140 192.168.2.50

10. Infrastructure NAS avec TrueNAS

Je test sur un poste client l'accès au nas depuis l'explorateur de fichier

On a bien accès au server depuis un poste



De plus la sauvegarde cloud du serveur de stockage se fait bien comme le montre la console AWS

Objets (1)	Ouvrir [2]
Les objets sont les entités fondamentales stockées dans Amazon S3. Vous pouver <u>S3</u> 2 pour obtenir une liste de tous les objets de votre compartiment. Pour que accéder à vos objets, vous devez leur accorder explicitement des autorisations. <u>Er</u>	z utiliser l' <u>inventaire Amazon</u> d'autres personnes puissent <u>n savoir plus</u>
Q Rechercher des objets en fonction du préfixe	< 1 > @
Nom ▲ Type ▼ modificatio ▼ Taille n n	✓ Classe de stockage
Image:	9.0 o Standard

11. Messagerie d'entreprise

La cliente se rendre sus zimbra pour pouvoir s'y connecter

Connexion		
- childright		
Utilisateur		
isabelle.moreau@)moreaunotaires.fr	
Mot de passe		
•••••	Afi	ficher
Connexion	Mémoriser mes valeur d'accès	s
	,	
Connexion	└ d'accès	
Version		
Défaut		~ (

Une fois ici on va se connecter et simplement faire un test d'envoi réception vers une adresse gmail, plus précisément la mienne

test	Boîte de récept	ion ×
MORE	AU Isabelle	
test	, Do:	MOREALL Icabella vicabella margau@margaunatairas fr
1051	De.	"iluge berrede", viluge berrede Ormeil eem:
	a:	liyes.berrada <liyes.berrada@gmail.com></liyes.berrada@gmail.com>
	Date:	19 mars 2025 23:13
(~	Objet:	test
	Envoyé par:	moreaunotaires.fr
	signé par:	moreaunotaires.fr
	sécurité:	Chiffrement standard (TLS) En savoir plus
	> :	Ce message a été classé dans les messages importants par Google

Nous pouvons voir que l'envoi de mail fonctionne bien.

Ainsi que la réception.

	ityes	
zimbra	2 2 3	Q. Rechercher dans bolte aux lettres
nessagerie		
NOUVEAU E-MAIL		🗸 Dale 🗸 🔸 🏟 🖬 Archiver 🎦 Déplacer 🗸 📳 Supprimer 🦁 Spam 🚥 Plus 🔠 Afficher 🗸
Boîte de réception Brouillons	Ilyes test test	1226 • test *
Envoyés Spam Corbeille		liyes «lyes beradağığınal com> 1226 A isabele moreau
+ Ajouter un dossier		🔦 Répondre 🌾 Répondre à tous 🛸 Faire suivre 🚥 Suite