

Rendu Projet Infra/SI

MODOLO Thomas / MATAS Lucas

Exploitation des outils/services mis en place

Sommaire

I - Introduction.....	p.2
II - Utilisation pfSense.....	p.2
II.1 Ajout d'une règle.....	p.2-4
II.2 Ajout d'un utilisateur au portail.....	p.5-6
III - Accès T-Pot.....	p.7-8
IV - Conclusion.....	p.9



I - Introduction

Dans ce document nous allons voir comment utiliser les deux services installé sur le serveur que nous avons créée. On commencera d'abord par pfSense ou je ferais une demonstration pour se connecter au portail captif, ajouter une règle...ect. En seconde partie nous verrons comment acceder a l'interface T-Pot.

II - Utilisation pfSense

II.1 - Ajout d'une règle

Avant de pouvoir vous connecter a pfSense nous allons devoir d'abord passer par le portail captif pour avoir un accès a internet (meme si pfSense est en local).

srv-pfsense.home.arpa x Captive Portal Login Page x

192.168.10.54:8002/index.php?zone=portail_ekip&redirurl=http%3A%2F%2Fdetectportal.firefox.com%2Fsuccess.txt#terms

You must log in to this network before you can access the Internet.

DOR DADA RECORDS

First Authentication Method

User

Password

Second Authentication Method

User

Password

☐ I agree with the terms & conditions

Login

Made with ♥ by Netgate

User01
Passw0rd

Toutes les règles peuvent être modifier ici :

Firewall / Rules / WAN

Floating WAN LAN DMZ

Rules (Drag to Change Order)

States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
✗ 0/8 KIB	*	RFC 1918 networks	*	*	*	*	*	*	Block private networks	⚙️
✗ 0/0 B	*	Reserved Not assigned by IANA	*	*	*	*	*	*	Block bogon networks	⚙️

No rules are currently defined for this interface
All incoming connections on this interface will be blocked until pass rules are added. Click the button to add a new rule.

↑ Add ↓ Add 🗑️ Delete 💾 Save ➕ Separator

Voici la liste des règles, c'est ici où tout se passe

L'ordre est important car plus une règle est haute dans la liste plus elle sera prioritaire.

Firewall / Rules / LAN

Floating WAN LAN DMZ

Rules (Drag to Change Order)

States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
✓ 2/220 KIB	*	*	*	LAN Address	443 80	*	*	*	Anti-Lockout Rule	⚙️
✓ 0/0 B	IPv4 TCP	*	*	*	53 (DNS)	*	none			📌 ✎️ ☑️ 🗑️
✓ 0/0 B	IPv4 TCP	*	*	*	443 (HTTPS)	*	none			📌 ✎️ ☑️ 🗑️
✓ 0/0 B	IPv4 TCP	*	*	*	80 (HTTP)	*	none			📌 ✎️ ☑️ 🗑️
✓ 0/0 B	IPv4 TCP	*	*	*	81	*	none			📌 ✎️ ☑️ 🗑️
✓ 0/0 B	IPv4 ICMP any	*	*	*	*	*	none			📌 ✎️ ☑️ 🗑️
✓ 108/48.93 MIB	IPv4 *	LAN net	*	*	*	*	none		Default allow LAN to any rule	📌 ✎️ ☑️ 🗑️
✓ 0/0 B	IPv6 *	LAN net	*	*	*	*	none		Default allow LAN IPv6 to any rule	📌 ✎️ ☑️ 🗑️

↑ Add ↓ Add 🗑️ Delete 💾 Save ➕ Separator

Ici c'est le menu d'ajout ou on va pouvoir tout paramétrer

Exemple ici avec une règle HTTPS

Action	<div>Pass</div>		
	Choose what to do with packets that match the criteria specified below. Hint: the difference between block and reject is that with reject, a packet (TCP RST or ICMP port unreachable for UDP) is returned to the sender, whereas with block the packet is dropped silently. In either case, the original packet is discarded.		
Disabled	<input checked="" type="checkbox"/> Disable this rule Set this option to disable this rule without removing it from the list.		
Interface	<div>LAN</div>		
	Choose the interface from which packets must come to match this rule.		
Address Family	<div>IPv4</div>		
	Select the Internet Protocol version this rule applies to.		
Protocol	<div>TCP</div>		
	Choose which IP protocol this rule should match.		

Source

Source	<input type="checkbox"/> Invert match	<div>any</div>	<div>Source Address</div> / <div></div>
<div> Display Advanced</div>			
The Source Port Range for a connection is typically random and almost never equal to the destination port. In most cases this setting must remain at its default value, any .			

Destination

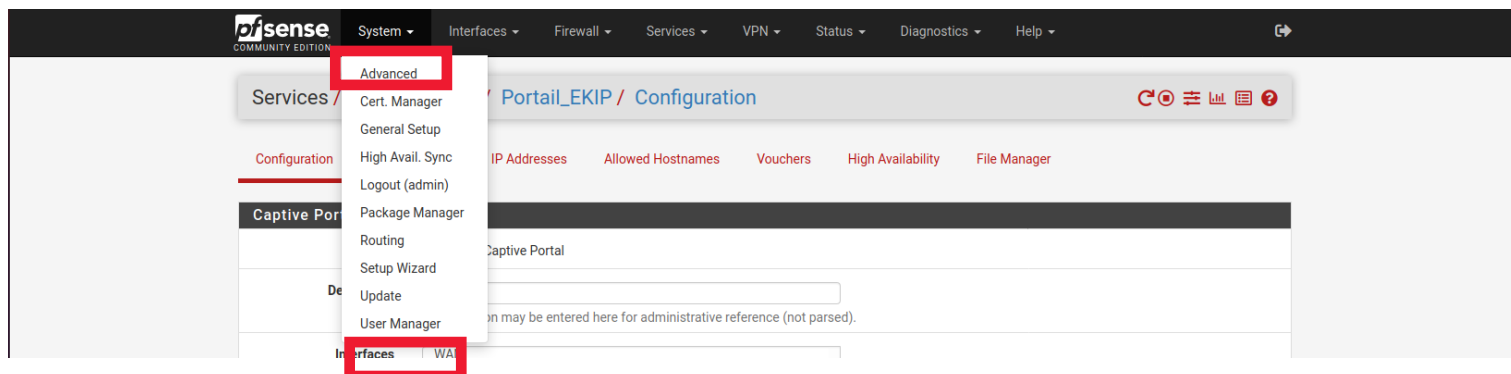
Destination	<input type="checkbox"/> Invert match	<div>any</div>	<div>Destination Address</div> / <div></div>	
Destination Port Range	<div>HTTPS (443)</div>	<div></div>	<div>HTTPS (443)</div>	<div></div>
	From	Custom	To	Custom
Specify the destination port or port range for this rule. The "To" field may be left empty if only filtering a single port.				

Extra Options

Log	<input type="checkbox"/> Log packets that are handled by this rule
Hint: the firewall has limited local log space. Don't turn on logging for everything. If doing a lot of logging, consider using a remote syslog server (see the Status: System Logs: Settings page).	

II.2 - Ajout d'un utilisateur au portail

Si vous êtes amené à devoir ajouter un utilisateur au portail voici comment faire



Voici la liste de tout nos utilisateurs

Users					
	Username	Full name	Status	Groups	Actions
<input type="checkbox"/>	User01	Lucas	✓	Portail_Group	Edit Delete
<input type="checkbox"/>	admin	System Administrator	✓	admins	Edit

[+ Add](#) [Delete](#)

Je vais en ajouter un pour montrer un exemple

Users					
	Username	Full name	Status	Groups	Actions
<input type="checkbox"/>	User01	Lucas	✓	Portail_Group	Edit Delete
<input type="checkbox"/>	admin	System Administrator	✓	admins	Edit

[+ Add](#) [Delete](#)

Nous devons simplement remplir les champs suivant :

- Username : avec le nom de notre utilisateur
- Password : mot de passe qui sera utilisé dès la connexion
- Full Name : Nom entier de la personne qui va utiliser ce user
- Group membership : groupe dans lequel va etre l'utilisateur

Voila, remplir ces champs suffiront amplement.

Users Groups Settings Authentication Servers

User Properties

Defined by USER

Disabled ☐ This user cannot login

Username

Password

Full name
User's full name, for administrative information only

Expiration date
Leave blank if the account shouldn't expire, otherwise enter the expiration date as MM/DD/YYYY

Custom Settings ☐ Use individual customized GUI options and dashboard layout for this user.

Group membership

Not member of

Member of

[» Move to "Member of" list](#) [« Move to "Not member of" list](#)

Hold down CTRL (PC)/COMMAND (Mac) key to select multiple items.

Certificate No private CAs found. A private CA is required to create a new user certificate. Save the user first to import an external certificate.

Full name

Status

Groups

Lucas



Portail_Group

Jazone



Portail_Group

System Administrator

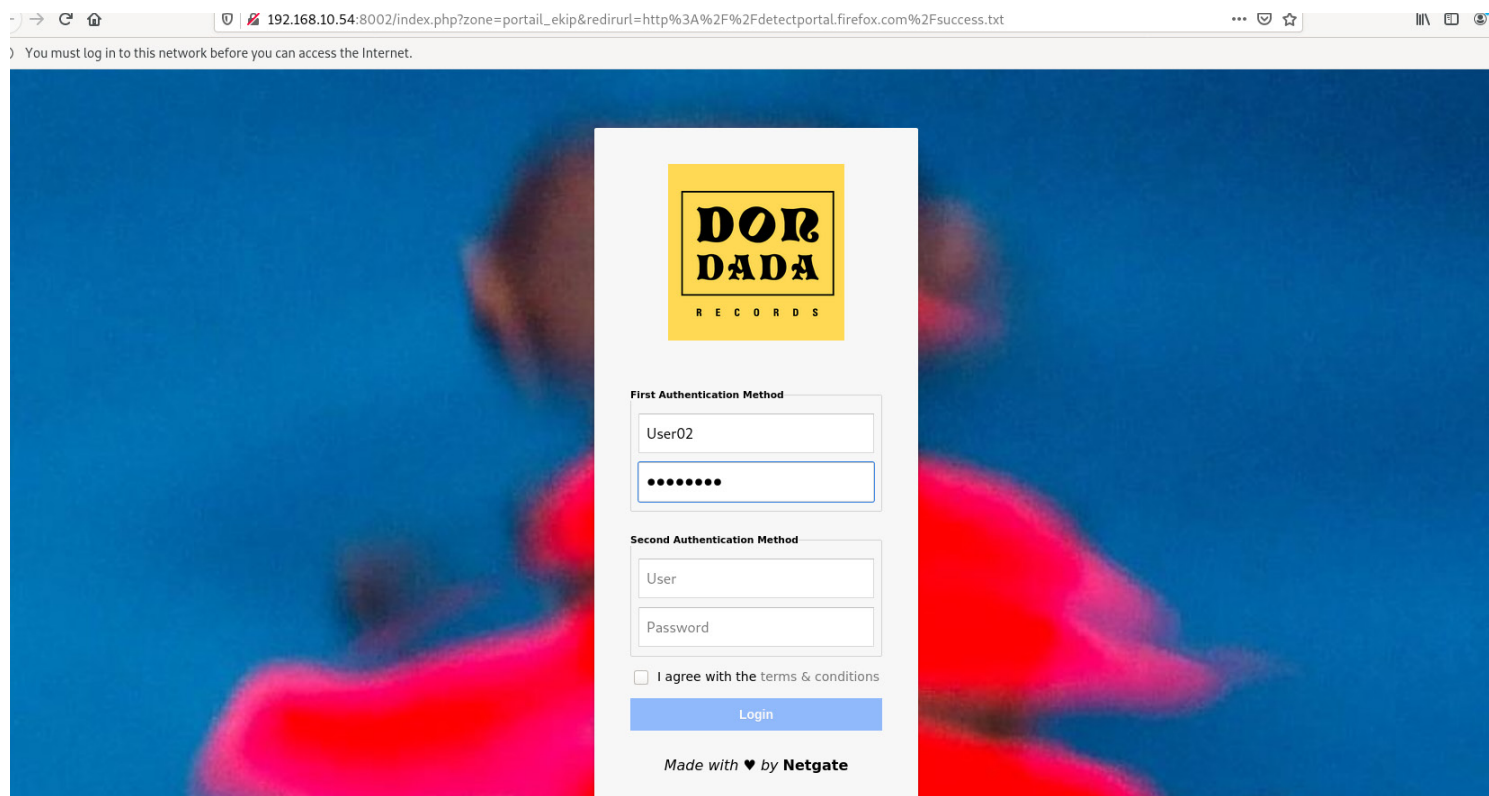


admins

III - Accès T-Pot

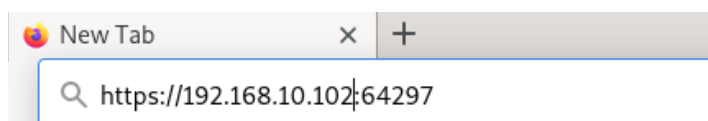
Pour accéder à T-Pot il faudra utiliser la machine sous debian.

Il faudra ensuite se connecter au portail captif et nous allons en profiter pour tester le compte que nous venons de créer.



Le compte fonctionne bien, on a donc un accès à internet sur la machine.

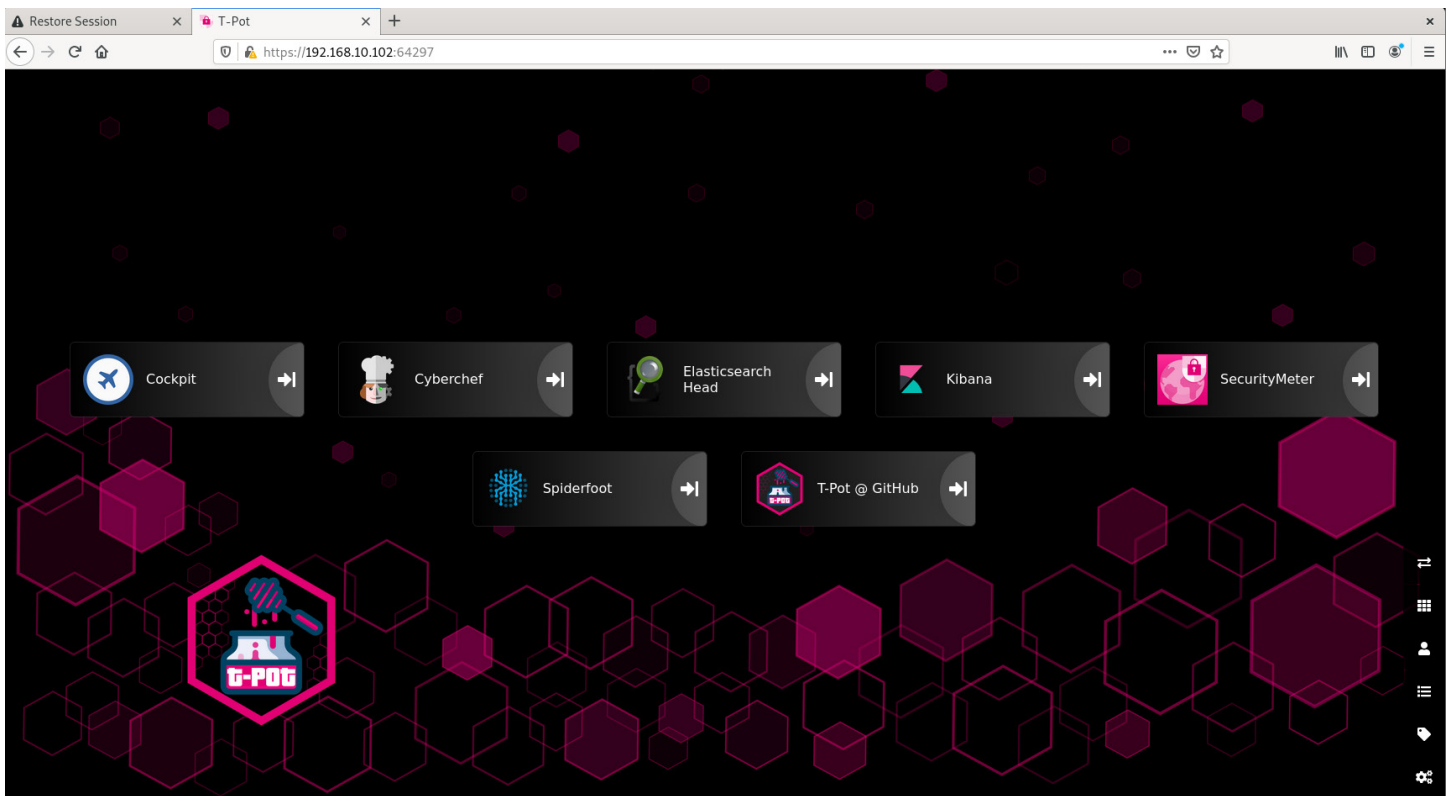
Ensuite il suffit de rentrer l'adresse suivante (composée de l'adresse IP de notre machine) dans notre navigateur pour accéder à l'interface T-Pot



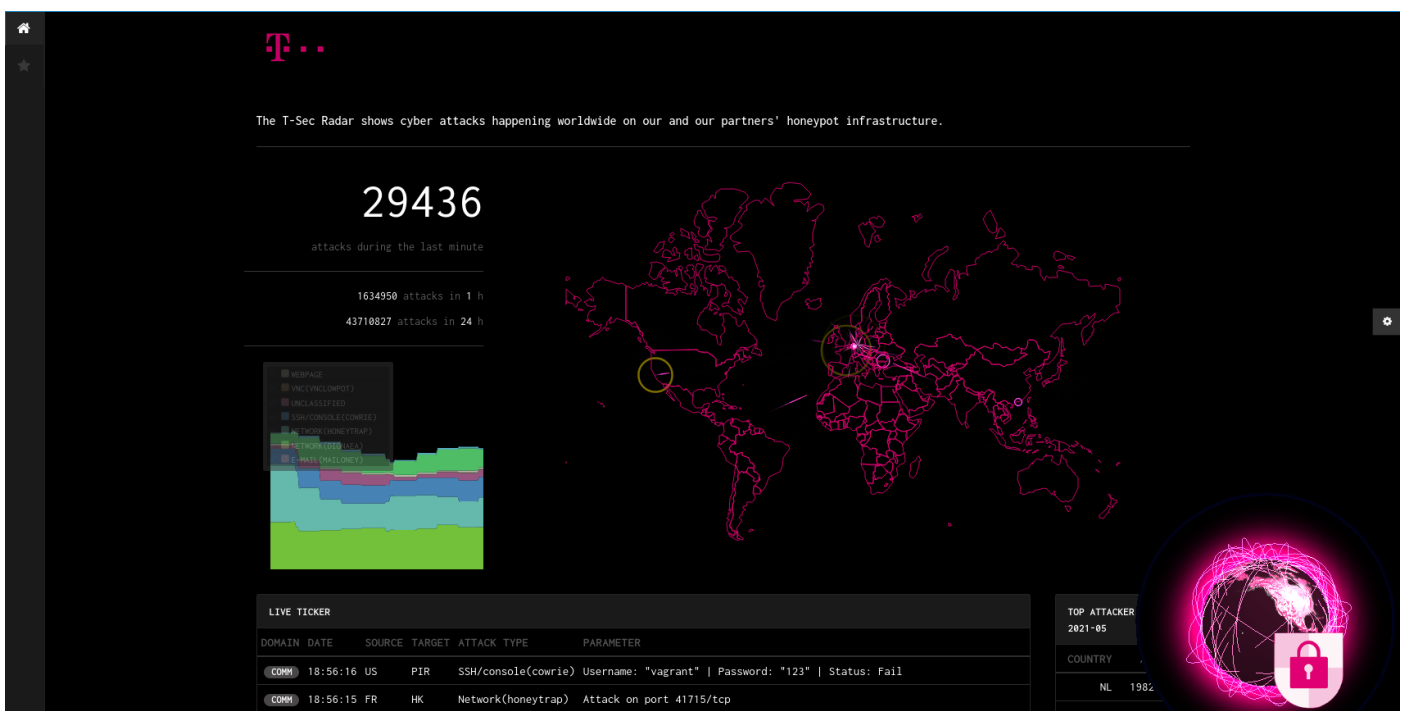
Ensuite il faut rentrer les information qui on été configurée dans le dossier technique :

- login : webtsec
- password : Passw0rd

Si les logs sont correct on arrive sur l'interface de T-pot



D'ici on pourra acceder a differente interfaces comme par exemple SecurityMeter qui va permettre de voir les attaque dans le monde en temps réel.



IV - Conclusion

Vous savez maintenant utiliser les quelques fonctionnalités/services mis(es) en place dans notre serveur et comment accéder à notre réseau.

Merci d'avoir lu