

Plate-forme d'entraînement de gestion de crise

Brandon Alves

INSA Lyon

INRIA

14 Juin 2021 - 13 Août 2021

- 1 Architecture du SI
- 2 Vulnérabilités & Attaques
- 3 Informations

- 1 Architecture du SI
- 2 Vulnérabilités & Attaques
- 3 Informations

Clients

- debian-client1 (Debian 10)
- debian-client2 (Debian 10) : machine du patron

Serveurs

- debian-web (Debian 9)
 - dans DMZ
 - LAMP
- debian-mail (Debian 9)
 - Poste.io
- debian-dns (Debian 9)
 - BIND9
- debian-file (Debian 9)

Routeur

- pfsense (Freebsd)
- 5 interfaces (WAN, administration, dmz, clients, services)
- Firewall pfSense
- DHCP

Attaquant

- debian-attacker (Debian 9)
- dans le réseau local de la machine roulant VirtualBox
- dispose de scripts ainsi que d'une interface web permettant de lancer différentes attaques

Administrateur

- debian-admin (Debian 10) : machine de l'administrateur

Architecture du SI

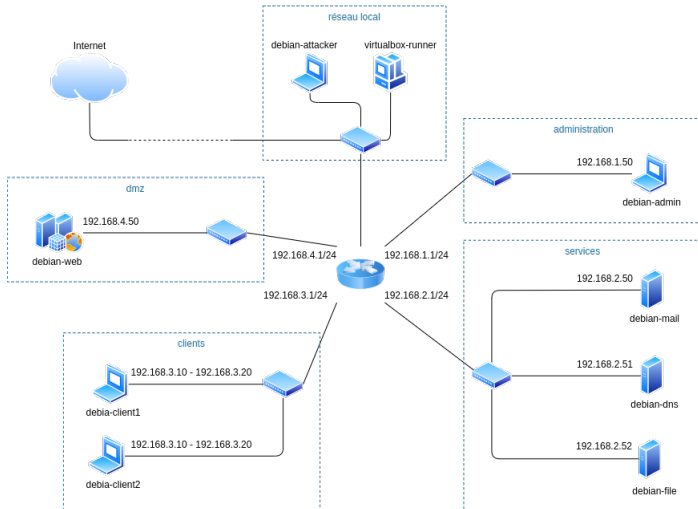


Figure – Architecture du SI

Déploiement de la plate-forme

Hébergement vs local

Hébergement

- Hébergé sur un serveur de l'INRIA ;
- Connexion via *Bureau à distance* ;
- Dépendant du réseau internet entre les machines et le serveur ;
- Puissance de calcul plus élevée ;
- Pas de conflit entre les différentes cellules de crises.

Local

- Indépendant du réseau internet entre les machines et le serveur ;
- Difficile de faire tourner plus d'une cellule de crise sur un laptop.

- 1 Architecture du SI
- 2 Vulnérabilités & Attaques
- 3 Informations

Vulnérabilités :

- Tout les comptes utilisateurs ont des mots de passe faibles ;
- Tout les comptes mails ont des mots de passe faibles ;
- RFI : vulnérabilité propre à Apache2 ;
- Aucun backup ;
- Ancun filtre contre les spams mis en place ;
- Firewall très permissif.

Attaque SSH par force brute

Script qui tente de se connecter en SSH à la passerelle avec un nom d'utilisateur et un mot de passe contenu dans une liste de mots de passe les plus fréquents. Lorsqu'une combinaison permet d'établir la connexion, celle-ci est enregistrée dans un fichier.

Attaque par déni de service (*Slowloris*)

Script qui envoie des requêtes HTTP partielles au serveur web, à intervalle régulier, afin de garder ses sockets ouverts.

Attaque par déni de service (*Ping*)

Script qui envoie des pings (requêtes ICMP) au serveur web à intervalle régulier obligeant celui-ci à répondre.

Attaque par déni de service (*UDP Flood*)

Script qui envoie un large nombre de paquets UDP à la passerelle à des ports aléatoires. Le serveur doit alors vérifier qu'une application est en train d'écouter ou non sur ce port et répondre avec des paquets ICMP.

Attaque par déni de service (*TCP SYN Flood*)

Script qui envoie une succession de requêtes SYN vers la cible, initialisant une connexion (three-way handshake). N'envoie pas le ACK final obligeant la cible à attendre un certain délai avant de fermer la connexion.

Défacement de site web

Script qui utilise une vulnérabilité RFI (Remote File Inclusion). Utilise le programme *weevely* pour se connecter au serveur.

Phishing

Script qui envoie des mails aux différents utilisateurs. Le mail demande de se connecter à un site en entrant ses identifiants. L'attaquant récupère ces derniers.

Ransomware

Script qui crypte le disque de la vm *debian-file*.

Spam (mail)

Script qui permet de spammer les différents utilisateurs par mail.

Spam (blog)

Script qui permet de spammer sur le blog de l'entreprise.

- 1 Architecture du SI
- 2 Vulnérabilités & Attaques
- 3 Informations**

Sur *debian-web*, *debian-dns*, *debian-mail*, *debian-file*, *debian-admin*,
debian-client1 :

login admin
password password

Sur *debian-client1* :

login mcurie	login lpasteur	login hpoincare
password fleur	password 12345	password motdepasse

Sur *debian-client2* :

login pdupont
password argent

Sur *debian-attacker* :

`login` attacker

`password` password

admin :

login admin@frenchleather.fr

password password

pdupont :

login pierre.dupont@frenchleather.fr

password argent

contact :

login contact@frenchleather.fr

password contact

mcurie :

login marie.curie@frenchleather.fr

password fleur

lpasteur :

login louis.pasteur@frenchleather.fr

password 12345

hpoincare :

login henri.poincare@frenchleather.fr

password motdepasse

Depuis l'extérieur, le SI est accessible via le protocole SSH sur la machine *debian-file* et la machine *debian-web*.

Le site internet de l'entreprise est accessible à l'url :
`http://www.frenchleather.fr`

Une interface web de messagerie est disponible à l'url :
`http://mail.frenchleather.fr`

FrenchLeather - Connexion avec Google

login frenchleathersa@gmail.com

password password123+

Attaquant - Connexion avec Google

login attacker554@gmail.com

password 123password+

Un tableau de bord est accessible à l'adresse `http://192.168.1.1` (login : *admin*, password : *password*).

Différents outils de monitoring :

- état des différentes interfaces ;
- informations générales sur l'état du routeur ;
- status des différents services du routeur ;
- statistiques sur les interfaces ;
- graphes représentant le trafic au niveau des interfaces ;
- pfTop : différentes connexions établies ;
- ...

Firewall : règles

`http://192.168.1.1/firewall_rules.php`

<input type="checkbox"/>	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description
<input type="checkbox"/>	✓ 0 / 0 B	IPv4 ICMP any.	*	*	*	*	*	none		
<input type="checkbox"/>	✓ 0 / 57 KiB	IPv4 TCP	*	*	192.168.4.50	80 (HTTP)	*	none		NAT NAT http
<input type="checkbox"/>	✓ 0 / 0 B	IPv4 TCP	*	*	192.168.4.50	8080	*	none		NAT NAT http
<input type="checkbox"/>	✓ 0 / 0 B	IPv4 TCP	*	*	192.168.4.50	22222	*	none		NAT NAT ssh
<input type="checkbox"/>	✓ 0 / 0 B	IPv4 TCP	*	*	192.168.2.52	22 (SSH)	*	none		NAT NAT ssh
<input type="checkbox"/>	✓ 0 / 0 B	IPv4 TCP	*	*	192.168.2.52	2222	*	none		NAT NAT ssh
<input type="checkbox"/>	✓ 0 / 0 B	IPv4 TCP	*	*	192.168.2.50	25 (SMTP)	*	none		NAT NAT smtp
<input type="checkbox"/>	✓ 0 / 0 B	IPv4 TCP	*	*	192.168.2.50	143 (IMAP)	*	none		NAT NAT imap

Figure – Règles filtrantes du firewall

`http://192.168.1.1/firewall_nat.php`








<input type="checkbox"/>		Interface	Protocol	Source Address	Source Ports	Dest. Address	Dest. Ports	NAT IP	NAT Ports	Description
<input type="checkbox"/>	<input checked="" type="checkbox"/>	 WAN	TCP	*	*	WAN address	80 (HTTP)	192.168.4.50	80 (HTTP)	NAT http
<input type="checkbox"/>	<input checked="" type="checkbox"/>	 WAN	TCP	*	*	WAN address	8080	192.168.4.50	8080	NAT http
<input type="checkbox"/>	<input checked="" type="checkbox"/>	 WAN	TCP	*	*	WAN address	22222	192.168.4.50	22222	NAT ssh
<input type="checkbox"/>	<input checked="" type="checkbox"/>	 WAN	TCP	*	*	WAN address	22 (SSH)	192.168.2.52	22 (SSH)	NAT ssh
<input type="checkbox"/>	<input checked="" type="checkbox"/>	 WAN	TCP	*	*	WAN address	2222	192.168.2.52	2222	NAT ssh
<input type="checkbox"/>	<input checked="" type="checkbox"/>	 WAN	TCP	*	*	WAN address	25 (SMTP)	192.168.2.50	25 (SMTP)	NAT smtp
<input type="checkbox"/>	<input checked="" type="checkbox"/>	 WAN	TCP	*	*	WAN address	143 (IMAP)	192.168.2.50	143 (IMAP)	NAT imap

Figure – Translations du firewall

Enregistrements DNS

\$ORIGIN frenchleather.fr.

Input	Type	Output
	SOA	debian-dns admin
	NS	debian-dns
	MX	10 debian-mail
debian-admin	A	192.168.1.50
debina-dns	A	192.168.2.51
debian-mail	A	192.168.2.50
debian-web	A	192.168.4.50
www	CNAME	debian-web
mail	CNAME	debian-mail
file	CNAME	debian-file
ns	CNAME	debian-dns

Table – Enregistrements DNS

http://192.168.1.1/

The screenshot displays the pfSense web interface dashboard. The top navigation bar includes menus for System, Interfaces, Firewall, Services, VPN, Status, Diagnostics, and Help. The main content area is titled 'Status / Dashboard' and is divided into several sections:

- System Information:** A table providing details about the system, including name, user, system type, BIOS version, and CPU type.
- Interfaces:** A list of network interfaces with their status (indicated by green up arrows) and IP addresses.
- Gateways:** A table showing gateway status, including RTT, RTTsd, Loss, and Status.
- Traffic Graphs:** A graph showing WAN traffic over time, with a legend for 'wan (in)' and 'wan (out)'.

System Information Table:

Name	pfSense.frenchleather.com
User	admin@192.168.1.50 (Local Database)
System	VirtualBox Virtual Machine Netgate Device ID: feb279621adaa11263eb
BIOS	Vendor: Innotek GmbH Version: VirtualBox Release Date: Fri Dec 1 2006
Version	2.4.5-RELEASE-p1 (amd64) built on Tue Jun 02 17:51:17 EDT 2020 FreeBSD 11.3-STABLE The system is on the latest version.
CPU Type	Intel(R) Core(TM) i7-9750H CPU @ 2.60GHz AES-NI CPU Crypto: Yes (inactive)
Kernel PTI	Enabled
MDS Mitigation	Inactive
Uptime	00 Hour 09 Minutes 06 Seconds
Current date/time	Wed Jul 21 16:47:07 UTC 2021
DNS server(s)	• 10.24.38.1 • 192.168.2.51 • 8.8.8.8
Last config change	Tue Jul 13 14:15:12 UTC 2021

Interfaces Table:

WAN	↑	1000baseT <full-duplex>	10.24.38.74
ADMINISTRATION	↑	1000baseT <full-duplex>	192.168.1.1
SERVICES	↑	1000baseT <full-duplex>	192.168.2.1
CLIENTS	↑	1000baseT <full-duplex>	192.168.3.1
DMZ	↑	1000baseT <full-duplex>	192.168.4.1
LAN	↑	1000baseT <full-duplex>	192.168.5.1

Gateways Table:

Name	RTT	RTTsd	Loss	Status
WAN_DHCP 10.24.38.1	1,364.8ms	1,899.1ms	5%	Offline

Traffic Graphs: A line graph showing WAN traffic. The y-axis represents traffic volume from 0.0 to 2.5M. The x-axis shows time from 05:10 to 07:12. The legend indicates 'wan (in)' (blue) and 'wan (out)' (orange). The graph shows very low traffic levels throughout the period.

Figure – Interface du routeur

<https://mail.frenchleather.fr/admin/rspamd/>

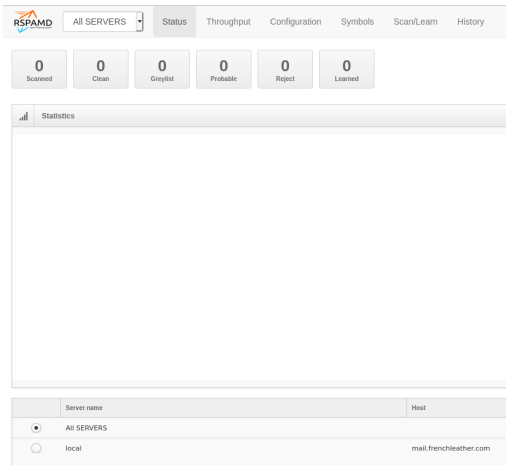


Figure – Interface de l'antispam mail

Site web de l'entreprise

<http://www.frenchleather.fr/>



French Leather SA

[Home](#) [Login](#) [Register](#) [About](#) [Join us](#)



French Leather SA 
@frenchleather

...

Les produits utilisés par French Leather sont 100% certifiés non toxiques pour l'environnement !



French Leather SA 
@frenchleather

...

French Leather met la sécurité de ses employés au centre !



French Leather SA 
@frenchleather

...

Tout nos partenaires sont fiers de travailler avec nous !

Figure – Page d'accueil du site de l'entreprise

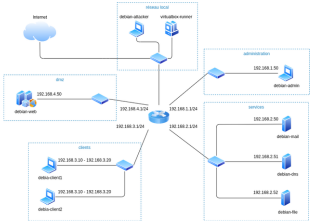
Interface de l'attaquant

http://<adresse_IP_de_la_machine_attaquante>/

Logs

Attacker IP address
10.24.38.75/24

SI schema



Nmap output

```
Starting Nmap 7.40 ( https://nmap.org ) at 2021-07-21 16:53 CEST
Nmap scan report for 10.24.38.1
Host is up (0.039s latency).
Nmap scan report for 10.24.38.64
Host is up (0.057s latency).
Nmap scan report for 10.24.38.67
Host is up (0.057s latency).
Nmap scan report for 10.24.38.74
Host is up (0.0023s latency).
Nmap scan report for 10.24.38.75
Host is up (0.00822s latency).
Nmap done: 256 IP addresses (5 hosts up) scanned in 3.91 seconds
```

Attacks

Refresh

Target IP

Set

Ransomware

Run

Denial of Service

Slowloris

Run

Ping of Death

Run

SSH Brute Force

Username

admin

Password list

French passwords top 1000

Run

Mail Spamming

Figure – Interface de l'attaquant

- Sur chaque machine, les commandes tapées sont enregistrées dans `/home/admin/.history/history.txt` ;
- Pour le firewall, on peut voir sur l'interface web du routeur ce qui a été modifié ;
- Mesure du temps durant lequel le site web de l'entreprise est resté défacé ;
- Mesure du temps durant lequel le temps de réponse à une requête au site web est trop long (pour le DoS) ;
- Nombres d'identifiant de connexions découverts (par l'attaque SSH ou phishing)