

# Plate-forme d'entrainement de gestion de crise

Brandon Alves

INSA Lyon

INRIA

14 Juin 2021

# Table des matières

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

# Table des matières

- 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)

# Architecture du SI

## Routeur

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

## Attaquant

- debian-attacker (Debian 9)
- dans l'internet
- dispose de scripts permettant de lancer différentes attaques

## Administrateur

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

# Architecture du SI

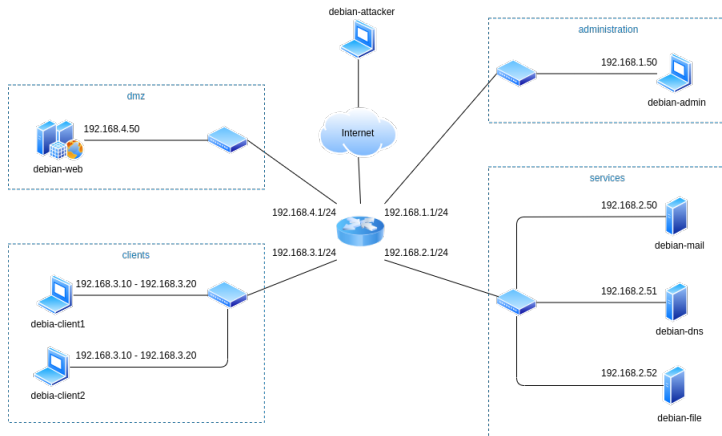


Figure – Architecture du SI

# Table des matières

- 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 ;
- Ancun filtre contre les spams mis en place ;
- Le firewall laisse tout passer.



## Attaque SSH par force brute

Script qui tente de se connecter en SSH à la passerelle avec pour nom d'utilisateur *admin* et pour mot de passe, un mot de passe contenue dans une liste de mots de passe français les plus courants. 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 les sockets de celui ci ouverts.

## Défacement de site web

Script qui utilise une vulnérabilité RFI (Remote File Inclusion). Utilise le programme *weeve/y* pour se connecter en SSH 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.

# Table des matières

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

# Comptes utilisateurs 1/2

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

login admin  
password password

Sur *debian-client1* :

login mcurie  
password fleur

login lpasteur  
password 12345

login hpoincare  
password motdepasse

Sur *debian-client2* :

login pdupont  
password argent

Sur *debian-attacker* :

login attacker

password password

admin :

login admin@frenchleather.com

password password

pdupont :

login pierre.dupont@frenchleather.com

password argent



mcurie :

login marie.curie@frenchleather.com

password fleur

lpasteur :

login louis.pasteur@frenchleather.com

password 12345

hpoincare :

login henri.poincare@frenchleather.com

password motdepasse

Toutes les machines sont accessible par le protocole SSH.

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

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












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

Figure – NAT

# Enregistrements DNS

\$ORIGIN frenchleather.com.

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

Un tableau de bord est accessible à l'adresse 192.168.1.1.

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 ;
- ...