

Plate-forme d'entraînement de gestion de crise

Brandon Alves, Antoine Boutet

INSA Lyon

INRIA

14 Juin 2021

Table des matières

- 1 Architecture du SI
- 2 Attaques
- 3 Informations
- 4 Sujet summer school

Table des matières

- 1 Architecture du SI
- 2 Attaques
- 3 Informations
- 4 Sujet summer school

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

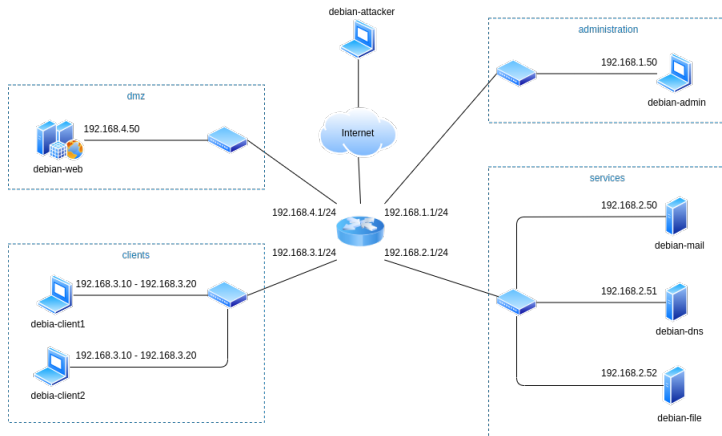


Figure – Architecture du SI

Table des matières

- 1 Architecture du SI
- 2 Attaques**
- 3 Informations
- 4 Sujet summer school

- Attaque SSH par force brute
- Attaque par déni de service (x2 dont *Slowloris*)

Table des matières

- 1 Architecture du SI
- 2 Attaques
- 3 Informations**
- 4 Sujet summer school

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

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											
<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	22 (SSH)	192.168.4.50	22 (SSH)	NAT ssh
<input type="checkbox"/>	<input checked="" type="checkbox"/>		WAN	TCP	*	*	WAN address	25 (SMTP)	192.168.2.50	25 (SMTP)	NAT smtp

Figure – NAT

Table des matières

- 1 Architecture du SI
- 2 Attaques
- 3 Informations
- 4 **Sujet summer school**

Description

- FrenchLeather SA
- tannerie
- région Lyonnaise
- travail comporte des risques pour les employés
- conditions de travail difficiles
- produits toxiques plus avantageux économiquement que produits bios

On peut imaginer ...

- vente en ligne → seveur web → DoS
- adresses de messagerie professionnel → piratage du compte du patron → chantage
- serveur de fichier ? des photos du patron avec sa maitresse ? → l'attaquant arrive à s'y introduire récupère les images et fait chanter
- serveur de base de données → contient : CA, nb de blessés, salaire, employés non déclarés, ...

Autres attaques

- injection SQL sur le site web de l'entreprise
- phishing par mail
- ransomware sur des données sensibles
- spyware

- <https://www.oodrive.com/fr/blog/securite/top-10-differents-types-cyberattaques/>
- <https://zeltser.com/malware-sample-sources/>