

Plate-forme d'entrainement de gestion de crise

Brandon Alves

INSA Lyon

INRIA

14 Juin 2021

Table des matières

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

Table des matières

1 Architecture du SI existante

2 Attaques existantes

3 Informations

4 Sujet summer school

Architecture du SI existante

Clients

- client1 (Debian 10)
- admin (Debian 10)

Serveurs

- web (Debian 9)
 - dans DMZ
 - LAMP
- mail (Debian 9)
 - Poste.io
- dns (Debian 9)
 - BIND

Routeur

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

Attaquant

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

Architecture du SI existante

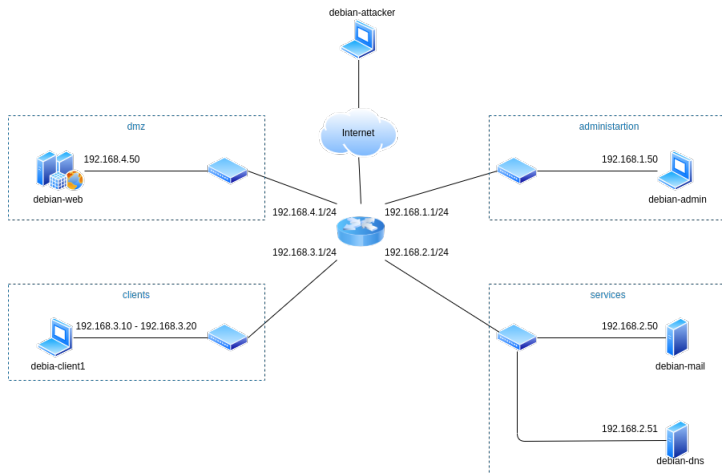


Figure – Architecture du SI

Table des matières

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

Attaques existantes

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

Table des matières

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

Sur chaque machine : 1 compte

- login = <nom de la machine>
- password = password

Firewall / NAT / Port Forward

Port Forward

1:1

Outbound

NPt

Rules

<div><div></div></div>			Interface	Protocol	Source Address	Source Ports	Dest. Address	Dest. Ports	NAT IP	NAT Ports	Description
<div><div><div></div><div>✓</div><div>↔</div></div></div>			WAN	TCP	*	*	WAN address	80 (HTTP)	192.168.4.50	80 (HTTP)	
<div><div><div></div><div>✓</div><div>↔</div></div></div>			WAN	TCP	*	*	WAN address	8080	192.168.4.50	8080	
<div><div><div></div><div>✓</div><div>↔</div></div></div>			WAN	TCP	*	*	WAN address	22 (SSH)	192.168.4.50	22 (SSH)	

Figure – NAT


Firewall / Rules / WAN										
Floating WAN LAN OPT1 OPT2 OPT3 OPT4										
Rules (Drag to Change Order)										
	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description
<input type="checkbox"/>	✓ 0 / 672 B	IPv4 ICMP <u>any</u>	*	*	*	*	*	none		
<input type="checkbox"/>	✓ 0 / 0 B	IPv4 TCP	*	*	192.168.5.2	80 (HTTP)	*	none		NAT
<input type="checkbox"/>	✓ 0 / 0 B	IPv4 TCP	*	*	192.168.4.50	80 (HTTP)	*	none		NAT
<input type="checkbox"/>	✓ 0 / 0 B	IPv4 TCP	*	*	192.168.4.50	8080	*	none		NAT
<input type="checkbox"/>	✓ 0 / 0 B	IPv4 TCP	*	*	192.168.4.50	22 (SSH)	*	none		NAT

Figure –

Firewall / Rules / LAN										
Floating WAN <u>LAN</u> OPT1 OPT2 OPT3 OPT4										
Rules (Drag to Change Order)										
<input type="checkbox"/>	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description
<input checked="" type="checkbox"/>	✓ 0 / 0 B	*	*	*	LAN Address	80	*	*		Anti-Lockout Rule
<input type="checkbox"/>	✓ 3 / 143.26 MiB	IPv4 *	*	*	*	*	*	none		Default allow LAN to any rule

Figure –

Firewall / Rules / OPT1										
Floating WAN LAN <u>OPT1</u> OPT2 OPT3 OPT4										
Rules (Drag to Change Order)										
<input type="checkbox"/>	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description
<input type="checkbox"/>	✓ 0 / 291.19 MiB	IPv4 *	*	*	*	*	*	none		

Figure –

Table des matières

- 1 Architecture du SI existante
- 2 Attaques existantes
- 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 → seueur 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/>