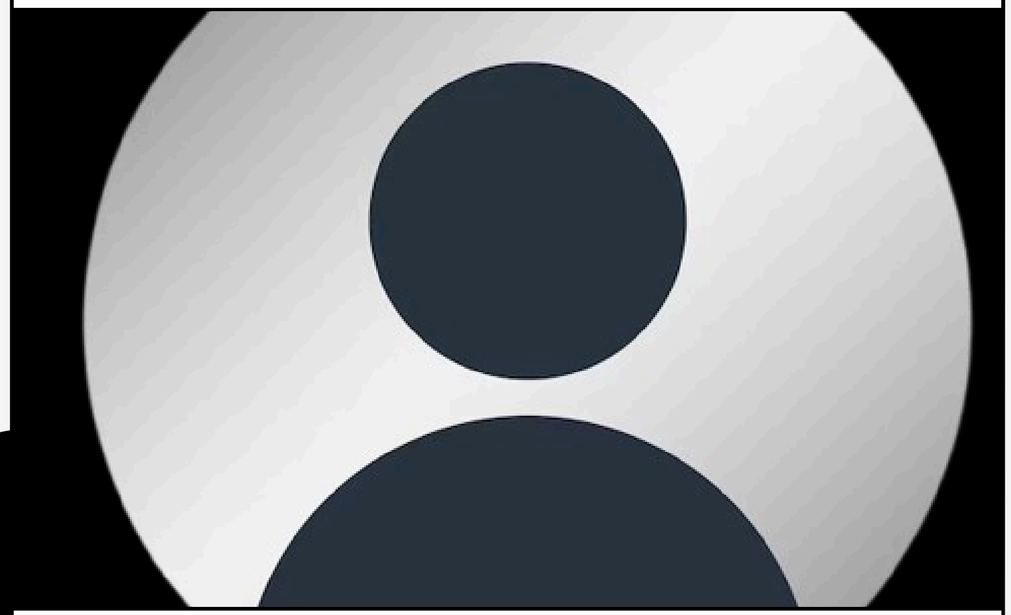
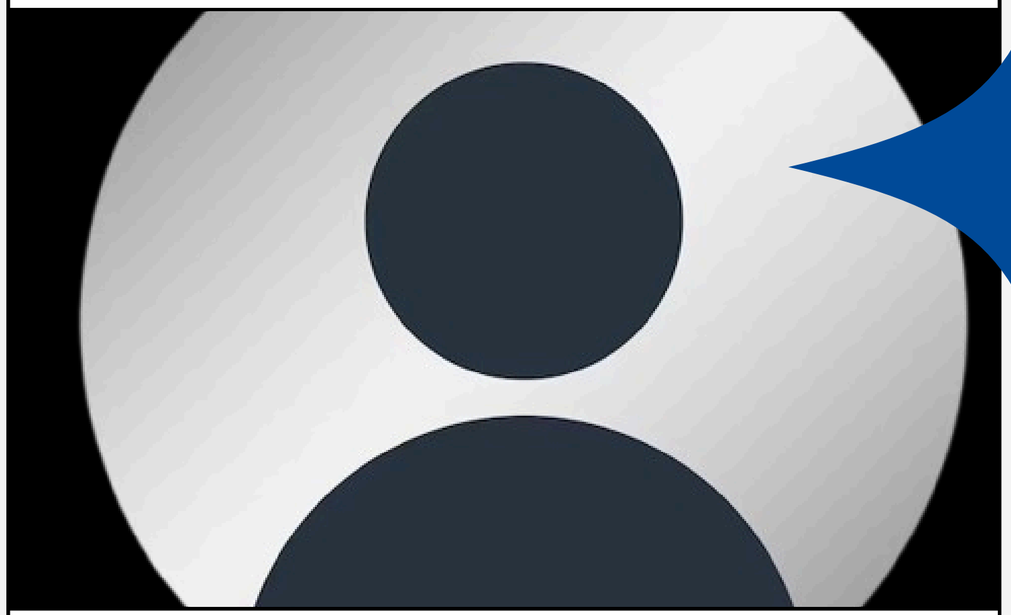
Notre Equipe

Marius Breinlen



Thomas Rubio



Réagir face à une cyber attaque

Recherche

SAE6.Cyber01

Sécuriser un système

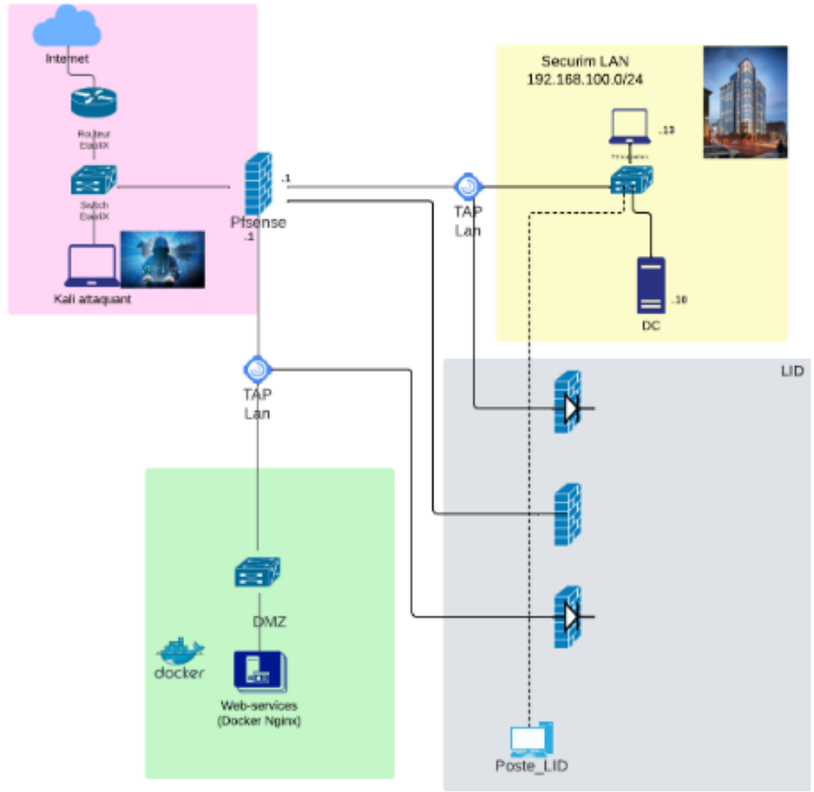
Présentation

générale du scénario

Dans un premier temps, nous jourons le rôle de la RED TEAM Nous attaquerons une entreprise telle que décrite dans le sujet. Et dans un second temps nous serons du coté de la BLUE TEAM en mettant en place un SIEM

Sommaire

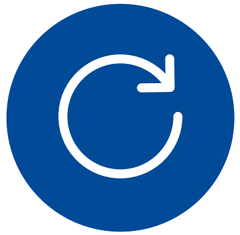
SECURIM



OSINT

FAILLES

RECONNAISSANCE



1

- http://securim.cfd
- Adresse
- Téléphone
- Email

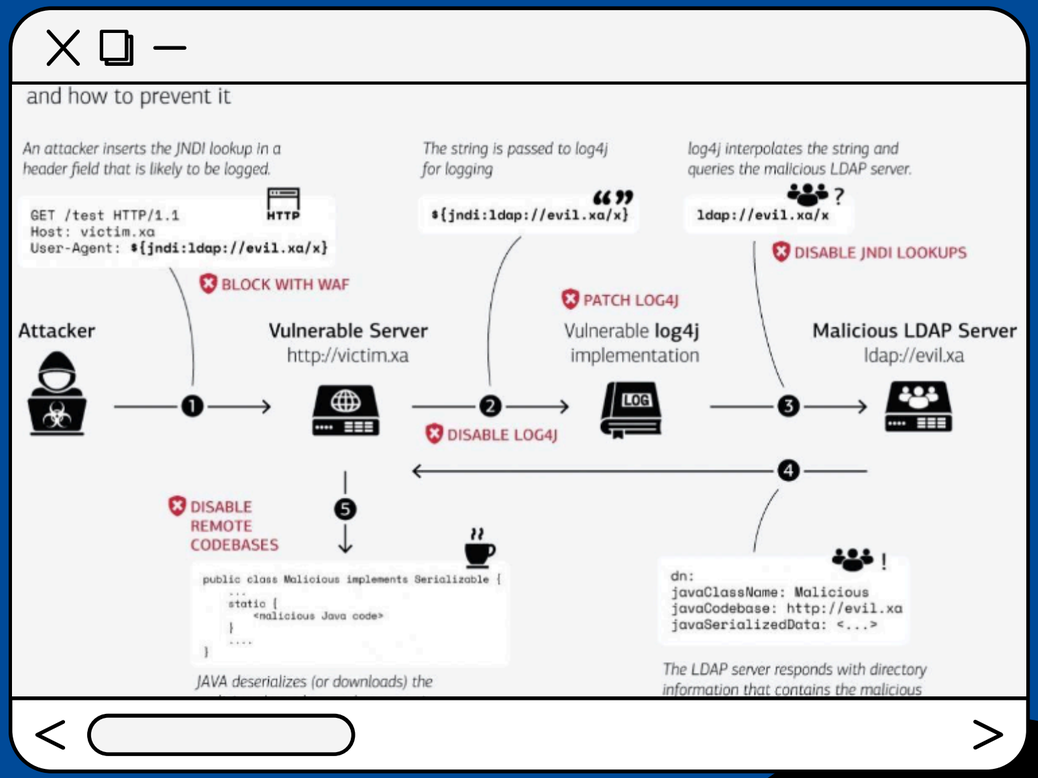
2

- Dirigent (Eric DUPUIS)
- Gilles RATAMACLAN
- Linkedin

3

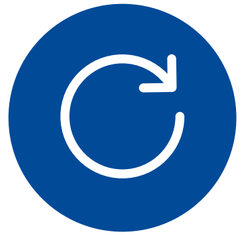
- Developpez.com
- Architecture
- Michel_MacCulligan
- Failles : Log4Shell

La vulnérabilité Log4Shell (CVE-2021-44228) dans la bibliothèque Log4j a été une faille de sécurité majeure découverte en décembre 2021. Elle permet à un attaquant d'exécuter du code à distance (RCE, Remote code Execution) en exploitant une fonctionnalité de Log4j qui accepte des données externes, notamment via l'API JNDI (Java Naming and Directory Interface). Cette vulnérabilité est particulièrement dangereuse car elle permet de faire exécuter du code arbitraire sur un serveur affecté en utilisant des requêtes malveillantes.



- Réalisation de l'attaque (RED TEAM)

RED TEAM



1

- Fuzzing
- Dirbuster
- Xhydra

2

- Log4Shell
- Exploitation

3

- Metasploit
- Meterpreter

Partie BLUE TEAM

Mise en place du SIEM/Agents
Deuxième Attaque

- Open source
- Détection des menaces
- Détection de vulnérabilités
- Support de nombreux formats de logs

- Consommation des ressources
- Courbe d’apprentissage
- Documentation parfois insuffisante
- Interface utilisateur

wazuh.

Mis en place des Agents

Select the package to download and install on your system:

LINUX	WINDOWS	macOS
○ RPM amd64	○ MSI 32/64 bits	○ Intel
○ RPM aarch64		○ Apple silicon
◉ DEB amd64		
○ DEB aarch64		

Run the following commands to download and install the agent:

```
wget https://packages.wazuh.com/4.x/apt/pool/main/w/wazuh-agent/wazuh-agent_4.11.0-1_amd64.deb && sudo WAZUH_MANAGER='192.168.100.30'
WAZUH_AGENT_NAME='web-service' dpkg -i ./wazuh-agent_4.11.0-1_amd64.deb
```

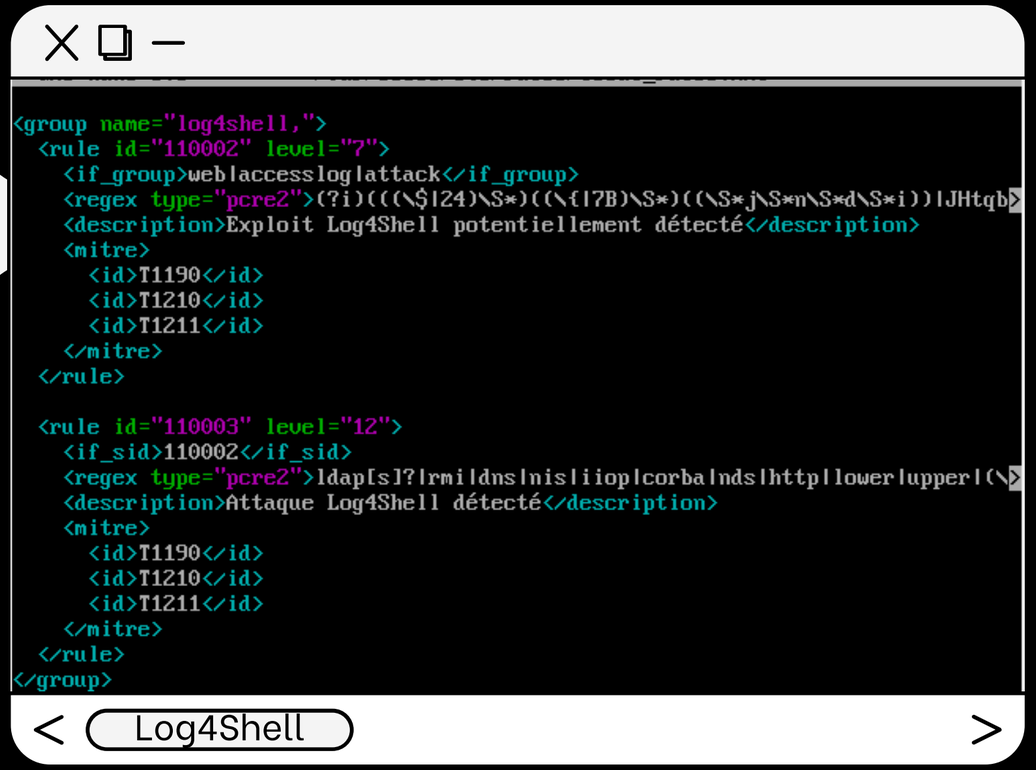
Start the agent:

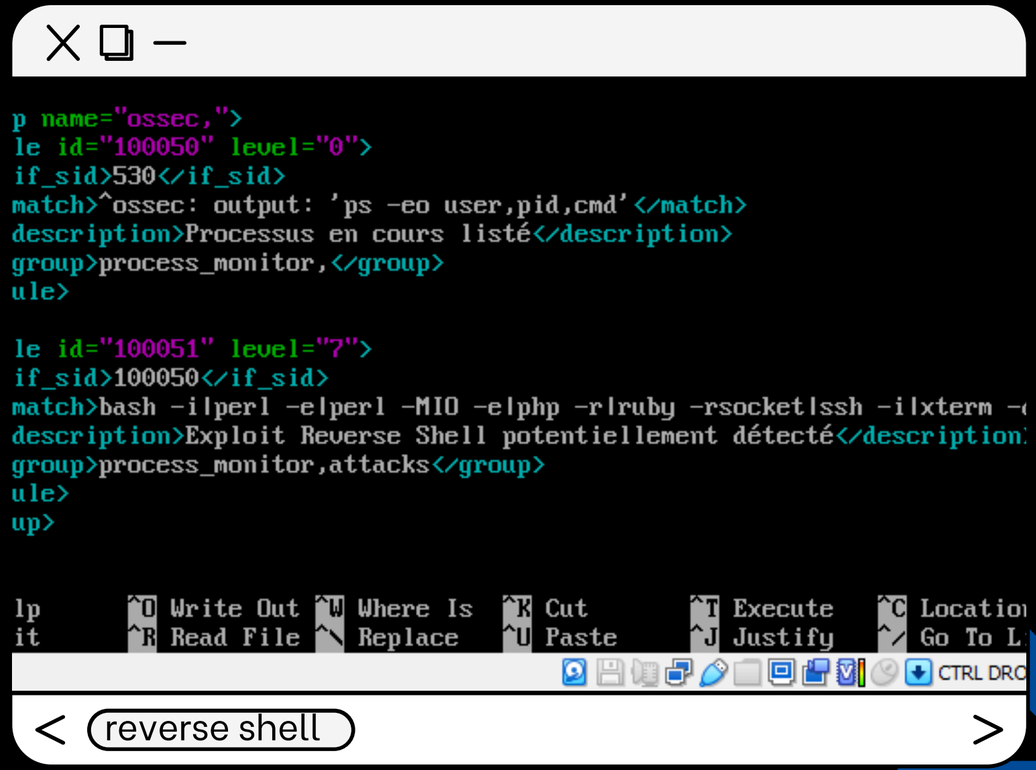
```
sudo systemctl daemon-reload
sudo systemctl enable wazuh-agent
sudo systemctl start wazuh-agent
```

Installation

Commande

Démarrage





Configuration des différentes règles

Log4Shell / Dirtypipe / Reverse Shell / Dirbuster

Logs des différentes attaques

Mar 19, 2025 @ 15:41:25.819 - Mar 20, 2025 @ 15:41:25.819

Export Formatted | 712 available fields | Columns | Density | 1 fields sorted | Full screen

timestamp	agent.name	rule.description	rule.level	rule.id
Mar 20, 2025 @ 15:41:18.9...	web-services	Attaque Log4Shell détecté	12	110003

Export Formatted | 712 available fields | Columns | Density | 1 fields sorted | Full screen

timestamp	agent.name	rule.description	rule.level	rule.id
Mar 20, 2025 @ 15:36:04.1...	web-services	Integrity checksum changed.	7	550
Mar 20, 2025 @ 15:36:00.7...	web-services	Dirty Pipe exploit activity detected (CVE-2022-0847)	12	700100

Export Formatted | 712 available fields | Columns | Density | 1 fields sorted | Full screen

timestamp	agent.name	rule.description	rule.level	rule.id
Mar 21, 2025 @ 13:29:30.5...	web-services	Scan DirBuster détecté	10	100100

Mar 20, 2025 @ 15:45:35.453 - Mar 21, 2025 @ 15:45:35.454

ort Formatted | 712 available fields | Columns | Density | 1 fields sorted | Full screen

timestamp	agent.name	rule.description	rule.level	rule.i
ar 21, 2025 @ 15:45:07.7...	web-services	Exploit Reverse Shell potentiellement détecté	7	1000

Conclusion

Ce projet nous a permis d’explorer en profondeur les méthodologies offensives et défensives en cybersécurité à travers une approche Red Team et Blue Team. En simulant des attaques réalistes, nous avons pu mettre en œuvre différentes techniques d’exploitation, allant de la reconnaissance OSINT à l’escalade de privilèges, en passant par des attaques ciblées comme Log4Shell.

Merci !

De nous avoir écoutés