**1. Reconnaissance Active Directory** :

* **Nmap** : Scanner de ports pour découvrir les services actifs sur le réseau.
* **Enum4linux** : Outil pour récupérer des informations sur les partages, les utilisateurs, et les groupes AD via SMB.
* **ldapsearch** : Outil pour interroger LDAP et récupérer des informations sur les objets AD.
* **BloodHound** : Cartographie des relations entre utilisateurs et machines dans AD, identifiant les chemins d'escalade de privilèges.
* **SMBMap** : Outil pour énumérer les partages réseau SMB et tester les permissions d'accès.
* **ADModule** : Module PowerShell pour interagir avec AD et récupérer des informations sur les utilisateurs et objets.
* **ldapdomaindump** : Dump d’informations AD via LDAP.
* **LDEEP** : Outil d'énumération et de cartographie des domaines et forêts AD.
* **ADRecon** : Génération de rapports sur la configuration AD.
* **ACLight** : Identification des mauvaises configurations d’ACL permettant des escalades de privilèges.

**2. Enumération d'Active Directory :**

* **PowerView** : Module PowerShell pour l’énumération AD (utilisateurs, groupes, permissions, etc.).
* **CrackMapExec** : Outil polyvalent pour l’énumération et l’exploitation d’AD via SMB, WinRM, et autres services.
* **ADRecon** : Génération de rapports détaillés sur les configurations AD.
* **Impacket** : Collection de scripts pour interagir avec SMB, LDAP, et d'autres protocoles pour énumérer des ressources et comptes.
* **WinPEAS** : Outil pour énumérer les vulnérabilités locales sous Windows et trouver des failles d’escalade de privilèges.
* **LDEEP** : Cartographie détaillée des forêts et domaines AD pour identifier des relations d'approbation.

**3. Attaques de mot de passe :**

* **Hydra / Medusa** : Outils de brute force pour casser les mots de passe via SMB, LDAP, RDP.
* **Responder** : Capture et empoisonnement de requêtes réseau pour voler les hashes NTLM.
* **Hashcat** : Outil de cracking de mots de passe, utilisé pour casser les hashes NTLM/Kerberos.
* **Mimikatz** : Outil pour extraire les informations d’authentification en mémoire (hashes, tickets Kerberos).
* **Rubeus** : Utilisé pour manipuler et abuser des tickets Kerberos (Pass-the-Ticket, Kerberoasting).
* **john** : Outil de cracking de mots de passe complémentaire pour Hashcat, avec des règles et dictionnaires.
* **Lsassy** : Extraction des credentials depuis le processus LSASS sur les systèmes Windows.

**4. Escalade de privilèges :**

* **PowerUp** : Outil PowerShell pour identifier les vecteurs d’escalade de privilèges dans AD.
* **Invoke-Kerberoast** : Script PowerShell pour lancer des attaques Kerberoasting et obtenir des tickets Kerberos de comptes de services.
* **SharpHound (outil utilisé par BloodHound)** : Collecte de données sur les relations entre les objets AD afin d'identifier les chemins d’escalade.
* **GPP Password** : Récupération des mots de passe stockés dans les objets Group Policy Preferences.
* **WinPEAS** : Scanning des failles locales pour l’escalade de privilèges, identifiant des configurations vulnérables.
* **Seatbelt** : Outil pour auditer la sécurité locale d’un poste Windows et identifier des potentielles failles d’escalade.
* **Windows Exploit Suggester** : Outil pour identifier les vulnérabilités connues d'un système Windows en fonction des correctifs manquants.
* **Potatoes (Juicy, Rotten, Sweet, etc.)** : Exploits permettant l'escalade de privilèges vers SYSTEM sur les systèmes Windows.

**5. Persistance :**

* **Mimikatz** : Extraction des tickets Kerberos pour créer des Golden ou Silver Tickets, permettant de maintenir l'accès.
* **DSInternals** : Outils pour manipuler directement les bases de données Active Directory, y compris les ACL (contrôles d’accès).
* **PowerSploit** : Framework pour persister via l’injection de DLL, la modification des ACL, ou l'ajout d'utilisateurs.
* **SharpPersist** : Outil .NET pour établir la persistance via des techniques variées (registre, services, etc.).
* **DonPAPI** : Extraction des informations sensibles stockées dans la "Protected User Data" (PAPI) sous Windows.

**6. Exploitation de vulnérabilités spécifiques à AD :**

* I**mpacket** : Contient des scripts pour des attaques spécifiques comme la synchronisation de la base AD (DCSync) ou la simulation de DC (DCShadow).
* **PetitPotam** : Exploite la vulnérabilité du protocole MS-EFSRPC pour forcer l'authentification NTLM des contrôleurs de domaine.
* **MS14-068 exploit** : Permet d’exploiter la vulnérabilité de Kerberos liée à l’élévation de privilèges.
* **Chisel** : Outil de tunneling pour contourner les restrictions réseau et établir une communication entre différentes machines lors des attaques.
* **Seth** : Exploit RDP man-in-the-middle pour capturer les informations de connexion.

**7. Post-exploitation :**

* **Mimikatz** : Extraction des credentials depuis la mémoire du contrôleur de domaine ou des autres machines sur le réseau.
* **CrackMapExec** : Outil pour le mouvement latéral, permet d'exécuter des commandes à distance via SMB, WinRM ou WMI.
* **PsExec** : Outil pour exécuter des commandes sur d’autres machines avec des privilèges administratifs.
* **Proxychains** : Utilisé pour forcer le routage des connexions réseau via un proxy (Tor, SSH tunnel) afin de masquer la source d’une attaque ou accéder à des services limités par des règles réseau.
* **evil-ssdp** : Outil pour réaliser des attaques MITM sur des réseaux vulnérables via le protocole SSDP.

**8. Exfiltration de données :**

* **Rclone** : Outil de synchronisation pour exfiltrer des fichiers vers des services cloud.
* **Powershell Empire** : Framework post-exploitation qui inclut des modules pour l’exfiltration discrète de données.
* **Netcat** : Outil simple pour transférer des fichiers de manière furtive.
* **Chisel** : Outil pour établir des tunnels TCP/UDP et exfiltrer discrètement des données, notamment dans les environnements restreints.